CAP

americanprogress.org

How To Regulate Tech

A Technology Policy Framework for Online Services

By Erin Simpson and Adam Conner November 2021

GETTY IMAGES/LANE TURNER

Contents

The positions of American Progress, and our policy experts, are independent, and the findings and conclusions presented are those of American Progress alone. A full list of supporters is available at https://www.americanprogress.org/c3-our-supporters. American Progress would like to acknowledge the many generous supporters who make our work possible.

Introduction and summary

Online services have evolved from novel communication tools to ubiquitous infrastructure for the United States' economy, democracy, and society. In 1995, 42 percent of U.S. adults said they had never heard of the internet.[1] Today, 85 percent of American adults are online every day, with nearly a third online "almost constantly."[2] This evolution has driven significant economic and social growth: Internet businesses now create 10 percent of U.S. gross domestic product (GDP),[3] on par with manufacturing, and nearly 15 percent of U.S. retail is e-commerce.[4] A majority of U.S. adults use social media, with large proportions using social media every day,[5] and many get their news through digital channels.[6] During the COVID-19 pandemic, nearly 93 percent of households with school-age children used some form of online "distance learning,"[7] and 71 percent of U.S. adults worked from home all or most of the time.[8] Online services have created tremendous benefits and new opportunities for expression. They have become an essential part of American lives and livelihoods.

Simultaneously, the growth of online services has created new inequalities, acute consumer protection issues, and troubling concentrations of power. Online service companies have produced substantial wealth, but these gains have failed to reach the American workforce more broadly.[9] Pervasive, ubiquitous digital surveillance has eroded Americans' civil liberties. Exploitation of people's data has created novel consumer threats around privacy,[10] manipulation of consumer behavior,[11] and discrimination.[12] Americans face these and other harms from online services, including but not limited to widespread fraud,[13] abuse of small businesses,[14] abuse of market power,[15] faulty algorithms,[16] racist and sexist technological development,[17] cybersecurity challenges,[18] threats to workers' rights,[19] curtailed innovation,[20] and challenges with online radicalization and misinformation.[21] These harms have affected all Americans but have had a disproportionate impact on low-income people, people of color, disabled people, and other systematically targeted communities. A persistent lack of transparency has compounded the public's ability to fully understand—let alone address—many of these challenges.

These problems are not inevitable. The economic, civil rights, privacy, and consumer protection harms from online services are not the necessary "cost" of flourishing online culture, commerce, and innovation. Rather, these harms are the result of business decisions and market failures, regulatory gaps and enforcement oversights, which have together produced an environment in which harmful and predatory practices among online services are industry standards.

Support for government action to regulate online services has grown as people's lives and livelihoods become more dependent on the internet.[22] Yet Congress has never passed a comprehensive framework for regulating online services, leaving federal oversight fragmented, incomplete, under-resourced, and unable to respond to emerging or even established harms in a timely manner. Considering the criticality of online services to not only the national economy but also the fabric of democracy and society, this level of risk has grown to be intolerable. In the robust progressive tradition of regulating industries in the public interest, wherein antitrust and regulation work together, online services too require new laws and regulatory authority backed by substantial resources. Multiple overlapping tools and specialist oversight are needed to identify and mitigate significant risks and prevent systemic problems.

Building on decades of incisive research on digital harms, experts have put forth stirring analyses of current problems and novel proposals for digital regulatory reform.[23] Others have powerfully explained the need for robust antitrust action, the case for structural separation as a key tool, and the challenges ahead.[24] Governments have laid the groundwork with efforts focused on pressing issues in digital marketplaces, from the U.S. House Antitrust Subcommittee's digital markets investigation and subsequently proposed legislation to new regulatory proposals from the European Union and the United Kingdom.[25]

The United States now has the opportunity to reestablish a public interest vision for online services. The 117th Congress can address several immediate issues by passing the bipartisan tech antitrust package[26] and taking up federal privacy legislation. It can make needed investments in agencies such as the U.S. Federal Trade Commission (FTC), which has existing authorities it can bring to bear to protect Americans online.[27] Reinvigorated antitrust enforcement can also deliver significant advances in competition and privacy. These are essential steps toward restoring competition, establishing privacy rights, and correcting some of the immediate online services harms. Yet even if these measures are implemented, significant gaps will remain in the government's fundamental ability to anticipate,

understand, and address the harms from all online services—not just those with monopoly power—while balancing the multiple, competing interests at the heart of many sociotechnical regulatory decisions.

The Center for American Progress seeks to advance a dynamic conversation about what is next in technology policy regulation. This report presents a new, common-sense framework for regulating online services of all sizes. These proposals are conceived as the next phase of restoring public interest oversight online—future action that is complementary to the steps the United States should take today. They aim to address current harms, create the capacity to prevent future issues, and promote innovation in the public interest for years to come. Building on existing work, this report makes five primary contributions:

1. Modeling what regulation could look like for all online services, beyond today's gatekeepers.
2. Advocating for a hybrid approach, encompassing baseline prohibitions of highly problematic practices in statute and a system of proactive, principles-based rule-making organized around the protection of civil rights and consumers, promotion of innovation and competition, and the need to balance occasionally competing interests among these values.
3. Proposing a unique opt-in regulatory tier specifically for online infrastructure companies, which require distinct treatment to protect the essential operation of information online.
4. Proposing a new test to contribute to the robust conversation around identifying digital gatekeepers in the United States.
5. Developing a cross-cutting approach that complements and strengthens existing sector-specific regulatory bodies through investigatory powers, referral powers, expert support, and regulatory coordination.

Historically, after-the-fact litigation has been too slow-moving to alone address online services harms. As Americans increasingly grapple with these harms and threats to the public interest, an ad hoc approach to online services is increasingly insufficient. To anticipate technology's evolution and balance difficult trade-offs, regulators should have proactive rule-making abilities to curb problems before or as they occur. New statutory prohibitions of problematic online services practices are likewise required to set clear rules of the road, especially for stable, long-standing online services markets. In combination, a hybrid regulatory approach backed by substantial resources and oversight powers is needed to tackle the range of public interest issues raised by online services.

This report proposes a high-level framework for thinking about the universe for regulatory action, the goals for regulation, potential tools to accomplish those goals, and ways to structure them. It envisions many potential pathways to actualizing this vision—a combination of new and existing statutes, new rule-making powers, and revived use of existing powers. The report also emphasizes that, given the inherent administrative challenges of regulatory oversight, use of structural separation regimes and clear statutory rules are preferable where appropriate and possible. Current FTC Chair Lina Khan and other experts have argued persuasively that structural separation approaches have particular relevance to digital platform competition, especially where platforms play a dual role of marketplace operator and competitor within the marketplace.[28] But this is not always feasible, especially in addressing issues that extend beyond the competitive harms from the largest players. This report conceptualizes a regulatory universe for all online services, encompassing potential structural separations, statutory prohibitions, new rule-making capacities, and increased capacity for oversight.[29]

This framework envisions several potential strategies for regulatory administration. Instead of preemptively determining which federal bodies should administer this approach, the authors hold that form should follow function. The report closes by discussing a set of administrative options but remains agnostic among those choices. Regardless of which agency path is chosen, significant future work will be required to overcome a range of administrability challenges that have limited the effectiveness of past efforts. Among them is designing robust safeguards against industry capture—wherein policymakers become unduly influenced by the industries they oversee—while also ensuring requisite specialized expertise. A range of technical and sociotechnical expertise—a term used to describe the blend of technical and social sciences skills needed to understand how people and technologies interact—is needed to holistically understand, anticipate, and remedy harms from online services for all Americans.

In defining the universe for regulatory action, this proposal focuses simply on providers of "online services," meaning products and services delivered through the internet. This straightforward approach acknowledges the increasingly digital nature of economic activity: Not all businesses that provide online services, for instance, are necessarily "tech companies." Therefore, a cross-cutting approach that focuses on the online service components delivered by many different types of providers is appropriate and complementary to existing, sector-specific regulations. This universe includes cloud infrastructure, artificial intelligence (AI) services, Internet of Things (IoT) devices, algorithmic decision-making systems, online advertising, app stores, media-sharing services, operating systems, search engines, e-commerce platforms, data analytics services, social media services, and more.

A focus on online services excludes core internet networking protocols—such as those managed through the Internet Engineering Task Force—as well as simple, static use of those protocols to display content, which does not rise to the level of service provision. Undoubtedly, there is a productive debate to be had on the optimal definitional approach.

This report proposes three complementary regulatory tiers to account for the wide variation in online services: online infrastructure, general online services, and gatekeepers. All online services, regardless of size, would fall into one of two categories: general online services, by default, or online infrastructure, which is opt-in and subject to regulator approval. Services that do not opt in to the online infrastructure tier are subject to any general online services rules; large, extremely powerful entities may additionally qualify as gatekeepers and face more tailored rules.

The online infrastructure tier—designed for infrastructural products such as web hosts, cloud services, and content delivery networks—is an opt-in regulatory category that aims to preserve online infrastructure by imposing public interest obligations such as common carriage, a requirement to deal fairly and equitably with all legal customers; nondiscrimination; and cybersecurity and other standards alongside greater regulatory stability and dedicated intermediary liability protections separate from Section 230 in the event that the law is changed. It provides baseline freedom of expression protections for legal content online and would enable a more focused discussion on carefully calibrated intermediary liability changes to higher-stack, consumer-facing services.

The general online services tier is designed for all other online services entities, regardless of size. It proposes prioritizing competition, civil rights, consumer protection, and privacy as the key principles for online services regulation—operationalized by dedicated statutes and accompanying rule-making capabilities guided by those principles and any process requirements enumerated by Congress. Clear, per se violations of rules can set a foundation for online services conduct. Additional principles-based rule-making would enable regulators to sustainably update and tailor protections to keep pace with emerging markets, balance competing interests within rule-making, and curb predatory practices on an ongoing basis. Proposed process requirements incorporate consideration of information diversity and pluralism, innovation, equitable growth, and representation of all participants in multisided markets. Equipped with significant technical expertise and research capacity, these regulators would be tasked with significant general oversight responsibilities over online services and also serve as specialist partners and referrers to other federal agencies.

The gatekeeper tier provides additional oversight for the largest online services companies whose dominance and power extend beyond a specific market, similar to recent work from the EU's Digital Markets Act and the tech antitrust package introduced in the 117th Congress. In order to determine gatekeeper status, this report builds on existing work to propose a new test of qualifying characteristics of dominant digital services. It proposes an array of specific thresholds for discussion, such as measuring significant market power through either a 30 percent or higher market share or persistently high Q ratios. For companies that qualify, this report envisions additional powers to complement existing antitrust enforcement. These include proactive rule-making powers and the ability to administer tailored remedies and sanctions, also guided by a narrow set of principles set forth by Congress. Akin to the systematically important financial institutions designation established by the Dodd-Frank Act,[30] designating powerful online services as gatekeepers that merit dedicated scrutiny enables regulators to look at business practices not only in isolation, but also in terms of what systemic risks they may pose to the economy and the public interest.

Amid growing demand for government action to address online harms and increasing regulatory action abroad, the United States must urgently pursue aggressive antitrust action, updated competition policies, and robust federal privacy laws and rules. Looking to the future, a comprehensive new regulatory approach for online services is critical. While the regulatory framework presented in this report would be a significant undertaking, the cost of inaction would be much greater. A government that cannot understand, much less anticipate, the dangers and potential of new technologies will increasingly fail the public over the coming decades. With that in mind, this proposal lays out commonsense ideas to enable effective democratic regulation of online services now and into the future.

This report proceeds by outlining the harms from online services—illustrating the economic, consumer protection, privacy, and civil rights issues they raise—and identifying the gaps in the current regulatory landscape for addressing those harms. Next, it proposes a three-tier regulatory strategy before diving into each of the three proposed categories: online infrastructure, general online services, and gatekeepers. Each section outlines the target entities, regulatory logic, and new tools proposed. The authors then discuss the proposals in the context of how they relate to a cross-cutting digital policy issue—how to handle the locus of problems grouped as "harmful online content"—by outlining potential ways that expanded regulatory capacity could contribute solutions. Finally, the report discusses options for administration—whether by expanding powers at existing agencies, creating a new agency or body, or using some combination of these approaches—and closes with a note looking to the future.

Defining online services

The focus of this proposal is online services, which refers to services and products delivered through the internet. Importantly, for the purposes of this report, it excludes: 1) the core set of protocols, standards, and networking architecture that constitute the internet itself, and 2) simple, static content displayed using those protocols, which does not rise to the level of service provision. Beyond that, the scope is deliberately straightforward: If a service does not work without the internet, it is considered an online service.

In technical terms, this encompasses services offered in the application layer of a traditional internet stack but generally does not encompass telecommunications or networking infrastructure further down the stack, such as physical networking infrastructure or internet service providers. In other words, online services picks up where Federal Communications Commission (FCC) internet regulation currently leaves off, focusing instead on "edge providers"—defined by the FCC as "content, application, service, and device providers, because they generally operate at the edge rather than the core of the network."[31] This definition includes cloud services, modern operating systems, app stores, search engines, social networking services, multimedia sharing services, online communications services, digital advertising infrastructure, IoT products, software as a service (SaaS) products, algorithmic decision-making services, and online marketplaces of all kinds. It would not include basic internet protocols, core standards, or display-only content put online; for example, a garden variety HTML display website[32] that lists and links text online would not be considered an online service. Though the vast scope of online services spans markets and regulatory areas, the commonalities are clear: Each is delivered over the internet, presents a regulatory gap, and faces common competition and consumer protection challenges that are endemic to online markets.

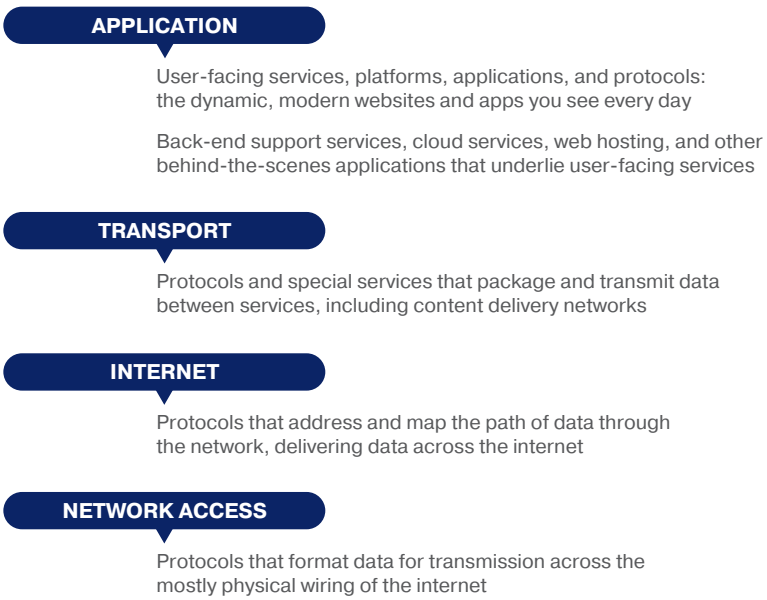
Conceptualizing the internet 'stack'

Conceptual models of the internet, including the internet protocol suite and the open systems interconnection model, use a "stack" framework to explain the operation of interconnected protocols that form the basis of the internet.[33] Rhetorically, the idea of the stack is used to discuss the range of technologies and protocols from the hard networking architecture at the bottom to the most consumer-facing services at the top. Figure 1 illustrates a simplified internet protocol stack. Many of the online services discussed in this report fall within the application layer of a traditional stack, although the authors also include some services that span application and transport layer services. Within the application layer, user-facing websites are conceptualized as higher up in the stack compared with the unseen cloud services or content delivery networks that underlie them. While the interconnections between middleware, software, and web applications are complex, various, and changing, the distinction between services that are consumer-facing or those that are not can be meaningful from a regulatory standpoint.

FIGURE 1

Visualizing the internet stack

Descriptions of internet layers from a user perspective



Source: For a wonderful introduction to layers of the internet and its mapping to the original Open Systems Interconnection model, the authors recommend ARTICLE 19, *How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship and Governance* (San Francisco: No Starch Press, 2021), pp. 76–77, available at https://nostarch.com/how-internet-really-works#content.

Framing this universe as "online services" seeks to reflect the reality that, while the scope and variety of online services will only increase, not all businesses or market participants should be considered tech companies or digital platforms. Rather, the business practices employed in the provision of online services have common elements that can be regulated with a common logic, even as they span unrelated industries. Roughly, these common elements include:

- **Common means of production:** Online services use computer science, data science, and digital design to build complex, interconnected systems and applications. They break data flows into bits and exchange them through internet protocols. Across different services, deep sociotechnical understanding of network and computer science is required for appropriate regulation.

- **Challenges endemic to many digital markets:** Online services operate at least partially in digital markets, which contain a unique mix of economic features that consistently produce competitive challenges. Numerous scholars and government bodies—such as experts at the University of Chicago Stigler Committee on Digital Platforms[34] and Ofcom, the United Kingdom's communications regulator[35]—have published reports outlining these barriers. They exist because of features inherent to digital markets such as network effects, economies of scope and scale, data advantages that give rise to asymmetry in competitively valuable information, first-mover advantages, and other well-understood economic forces.[36] This combination of factors makes markets prone to "tipping"—as firms compete for the market, one firm is likely to "win," and other firms will face extremely high barriers to entry. While specific remedies for competitive problems may vary by market, a common logic and language around balancing the risks, opportunities, and values in digital markets can help inform, improve, and deconflict regulatory responses across sectors.

- **Common societal shift:** Online services operate within and as part of a cultural and economic shift. Americans are increasingly grappling with the adoption, integration, adaptation, and refusal of online services in their day-to-day lives. The federal government must listen to and understand Americans' emerging logics and changing needs, taking a critical approach to claims of inevitability around adoption or specific directions for technical development.

The authors recognize the difficulty of balancing policy tensions and conflicting interests, as described in Ofcom's 2019 report on regulating online services:

> *Online services pose particular challenges for regulators. This is because of their global nature, the fast pace of change, the complexity of online business models, the scale of online content and the variety of services available online. The links that may exist between different harms can create overlaps and tensions between policy aims. These are challenges for existing regulators, as well as for any future regulation of online services being considered by Government.*[37]

While some online services markets are fast-moving or complex, others are stable or straightforward. The ubiquity of claims from industry—that their operations are too complicated to be appropriately regulated—presents an even stronger argument for an increase in the number of public servants who know the difference. Online services are not so complex as to be unregulatable, and opacity in their operations can be remedied.

There are meaningful definitional challenges to be worked out in this or other approaches.[38] However, these challenges must be overcome if the United States is to functionally address the multitude of harms occurring from the unchecked power of both new technologies and dominant gatekeeper platforms.

Understanding harms from online services

The growth of the internet has produced significant social, cultural, and economic benefits for the United States. Providers of online services have helped shepherd the internet from its infancy into a more accessible digital layer that interweaves with most Americans' lives on a daily basis. With the exponential growth of online services and their attendant benefits, however, a number of harms have also emerged, enacted or enabled by online services providers. While many Americans have grown up accepting these harms as a cost of engaging online, the harms generated by online services are not inevitable. Current problems are not necessary evils for the sake of digital innovation, and improved regulation has a dual role to play in promoting beneficial development and curbing predatory practices.

In order to support a vibrant, dynamic internet that serves the public interest, it is necessary to understand not just the benefits but also the harms from online services and the risks they pose to economic, social, and democratic health. These harms are salient and widespread, even where services are offered at low or no monetary cost to users—for example, free email or social networking platforms, which are subsidized by intensive data collection, online tracking, and targeted advertising. These harms tend to be disproportionately borne by marginalized groups—including people of color, low-wage workers, and women—whereas technology's benefits asymmetrically accrue to more privileged groups.[39] In aggregate, these issues amount to troubling threats to commerce, civil rights, and democratic function. To make these issues more legible to traditional regulatory approaches, they are grouped below into four overlapping and deeply interconnected areas: economic harms, privacy harms, consumer protection harms, and civil rights harms.

This survey of harms is necessarily incomplete. While a full examination of online harms is beyond the scope of this report, the limited information available also speaks to the profound asymmetry and lack of transparency in the online services space. This information asymmetry—the stark lack of data accessible to government and the public compared with the mountains of data held by digital platforms—is a persistent issue across different areas of harm. Indeed,

the harms described below may only be the tip of the iceberg. Researchers are starved for data on online harms and competition, and many of these issues have only come to light through formal government inquiries, whistleblowing, or intrepid investigative journalism.[40]

Economic harms

The proliferation of the internet and digital communication technologies have produced new and complex online businesses. The largest of these businesses have developed communication and information services that have become essential to billions of consumers and are protected from new competitors by powerful barriers to entry. As noted above, these barriers exist because of inherent features of digital markets such as network effects, economies of scope and scale, data advantages, first-mover advantages, and other economic forces.[41] They have been preserved, reinforced, and compounded over time by strategic acquisitions and successful efforts by firms to foreclose nascent competitors and discourage competitive threats,[42] resulting in traditional problems arising from a lack of competition—higher prices, lower quality, and less innovation. In markets dominated by an incumbent digital gatekeeper, the threat of the dominant firm copying or killing any new innovations results in decreased investment, deterrence of entry, and decreased innovation in the digital platform industry.[43] Big tech mergers likewise have adverse competitive effects on growing markets,[44] and incumbent firms may acquire younger firms explicitly to curb innovation that threatens their position.[45] More than 80 percent of Americans believe acquisitions from large online platforms are likely unfair and undermine competition.[46] But with few alternatives, high switching costs—for example, the difficulty or inability to move personal data when shifting to a new service—and extremely powerful network effects mean that American consumers have a limited ability to "vote with their clicks." Even with great effort, it is difficult to avoid using major firms; journalist Kashmir Hill described her experiment living without any services from five nearly inescapable technology companies as "hell."[47] This lack of choice further removes incentives for dominant players to innovate to improve services.

Centralization of research and development (R&D) resources at dominant firms may additionally result in selective or reduced innovation. A lack of external competition, for instance, discourages innovation,[48] and internal research that threatens dominant business lines is often avoided, hidden, or systematically challenged.[49] There may be significant opportunity costs to having only a few big U.S. technology companies driving the direction of technological progress

for the economy more broadly, especially given the competitive incentives for dominant firms.[50] Experts have also raised concerns about the national security risks of relying on only a handful of dominant global technology companies that may not prioritize U.S. national security interests and do not have sufficient competitive incentives to ensure continued innovation, performance, and efficiency.[51] There is nothing wrong with firms pursuing innovations entirely compatible with their business models. But when such R&D capacity is concentrated among only a few major technology firms with similar incentives and limited demographic diversity, there is cause for concern about whether these innovations will benefit low-wage workers, address climate change, and benefit the public interest, or whether they will continue to concentrate America's R&D efforts around issues such as selling online advertising.[52]

A lack of competition also produces pricing harms, even when the direct consumer price is zero or the upfront consumer price is competitive. Indeed, a multisided platform—for example, a website that brings together consumers, business users, and advertisers and provides a platform for sales and interaction—may charge fees to business users that are directly passed on to consumers down the line. Consumers who enjoy low prices from digital giants today might also face higher prices in the future: Incumbent firms may use price-cutting strategies or subsidies to kill potential competitors and build or maintain market power, producing lower prices in the near term but ultimately resulting in higher prices and lower quality. Amazon, for example, dropped its diaper prices by more than 30 percent, effectively curbing the growth of online retailer Diapers.com and undercutting the company whenever it dropped prices.[53] Through cross-subsidization with other business lines, Amazon was able to absorb losses on baby products in the short term, "no matter what the cost,"[54] in order to maintain its dominant market position and price-setting ability in the long term, catalyzing the forced sale of the once-burgeoning diaper retailer. In her landmark paper "Amazon's Antitrust Paradox," Lina Khan argued, "The fact that Amazon has been willing to forego profits for growth undercuts a central premise of contemporary predatory pricing doctrine, which assumes that predation is irrational precisely because firms prioritize profits over growth."[55] While many markets experience this kind of short-term corporatism, its effects in digital markets are more harmful. As noted earlier in this report, digital markets are prone to tipping, wherein one firm is likely to "win" and maintain most of the market after gaining an early lead. Firms then leverage existing dominance for further expansion, tipping, and entrenchment in adjacent markets, making the economic consequences of unchecked predatory behavior particularly high.

American small businesses are likewise harmed by a lack of competition among digital platforms. Facing few alternative choices, high switching costs, and little power to change platform conditions, American small businesses face a high degree of platform precarity: increased risk due to heavy reliance on a handful of dominant platform services over which they have little influence or recourse if problems arise, even when platforms are treating them unfairly. Dominant platforms use this knowledge to extract rent in the form of unfavorable pricing, terms, agreements, and more;[56] examples include third-party business users such as restaurants using food delivery apps, third-party retailers creating storefronts on major online retail services, and content creators monetizing their video or audio content. Small and medium-sized businesses are forced to invest significant resources to compete effectively on online platforms, but sudden, unilateral changes in terms,[57] ranking,[58] pricing,[59] design, or a sudden suspension[60] can wipe out the value of a business' investment. Even getting out of these service arrangements can be costly: Cloud services, for example, may make it cheap to transfer data into the service but charge ultra-high rates for egress fees to leave a service.[61]

American small businesses face a high degree of platform precarity: increased risk due to heavy reliance on a handful of dominant platform services over which they have little influence or recourse if problems arise, even when platforms are treating them unfairly.

Worse, platforms may exploit data about a business' sales and products to develop copycat products and undercut small businesses,[62] potentially even self-preferencing first-party services through pricing, data, design, ranking, and bundling strategies.[63] Increasingly, dominant platforms' theft of content threatens internet openness and undermines small or growing firms.

American workers are also harmed under the status quo. When dominant firms drive out competitors and achieve market capture, firms become labor monopsonists,[64] meaning that they acquire disproportionate power to set and decrease wages because they face little competition that might otherwise motivate a competitive wage and safe working conditions.[65] Worker abuse is easy to disguise through the ubiquitous use of opaque business software and algorithmic management systems, which may rely on surveillance to monitor and shape

worker behavior.[66] While some of these issues can be addressed through updating and robustly enforcing labor laws, the competitive failings of digital markets will continually put downward pressure on wages and working conditions in monopsonized labor markets.

A persistent lack of transparency and data asymmetry exacerbate these problems. While workers or business users may feel that abuse is occurring, it is difficult to investigate problems without greater data access. These issues are of growing importance to Americans, with 81 percent of voters saying they are "concerned about consolidation among Big Tech corporations hurting small businesses and consumers."[67]

Privacy harms

Historically, while businesses such as telephone networks have also been protected by strong network effects and high barriers to entry, online service providers are unique in that many also surveil their consumers—sometimes without consumers' awareness—and use the information they gather to manipulate user behavior to increase usage and revenue. Other companies then buy this information from surveillant firms, develop predictive statistical models, and sell those models for wider use. The application of these models materially affects peoples' lives in ways that are often hidden from them; the resulting invasions of privacy and invisible impacts on people's health, economic prospects, education, and liberty have produced novel forms of harm to society. Due to the complex and sometimes deliberately obscured workings of online services, it can be difficult or impossible for individuals to understand, address, or even identify the origin of these harms—let alone choose a better option if one is available.

Unwanted and invasive data collection, processing, and sale have become standard practice in online services industries, and Americans are overwhelmingly concerned about the data platforms hold.[68] The scope and detail of corporate data collection and consumer surveillance are astounding. For example, Google reportedly has acquired information on 70 percent of all U.S. credit and debit card transactions[69] to combine with its detailed user profiles. An entire industry has grown around creating and selling constant, unwanted records of billions of people's locations at scale in gross detail:[70] One analysis found that location trackers in common, innocuous mobile phone apps were updated more than 14,000 times per day, identifying individuals' location down to within only a few yards.[71]

These data are profoundly abused. Companies collect consumer contact information and movements without consent;[72] perpetuate the pretense that consumers give informed consent with the click of "I agree";[73] use deceptive disclosures and settings to trick consumers into allowing data sharing with third parties;[74] track consumers' location within a few feet inside their homes;[75] track consumers' location even after tracking is turned off;[76] develop new products using consumers' personal emails, photographs, and conversations;[77] track people's ovulation data without consent;[78] and then too frequently fail to secure the massive troves of intimate and valuable data they acquire. It is not just dominant firms engaging in this behavior: In some cases, small businesses and third-party data buyers are the worst abusers of consumer privacy.[79]

Indeed, privacy harms are acute in combination with competitive harms. Experts have shown that firms that achieve market dominance and successfully suppress competitive threats are able to lower privacy protections in order to pursue and extract greater data gains from consumers.[80] Consumers, without a reasonable choice of substitutes, are forced to put up with suboptimal privacy protections and even privacy invasions. Within digital markets, experts including Howard Shelanski have argued that "one measure of a platform's market power is the extent to which it can engage in [data usage that consumers dislike] without some benefit to consumers that offsets their reduced privacy and still retain users."[81] As illustrated by Dina Srinivasan, Facebook's pivot away from privacy protection toward privacy exploitation upon achieving monopoly status is emblematic of this power, with consumer data extraction constituting part of the firm's "monopoly rent."[82]

The collective costs of individual privacy incursions, of which consumers are often unaware, are staggering. These costs are not just economic—although billions of dollars have been lost through corporate negligence to protect these data, especially sensitive information concerning individuals' credit, finances, and identity[83]—but also democratic, social, and humanitarian. Troublingly, Americans have changed their social and political behavior because they know they are being watched by corporations and law enforcement.[84] Ambient surveillance has chilling effects on expression, civil liberties, and freedom of movement, particularly for Black and Hispanic communities that are persistently oversurveilled and overpoliced.[85] Americans' personal interactions, behavior, and political activity have become commodities to be tracked without consent, bought, and sold. As companies reach beyond merely advertising to manipulating people's behavior,[86] the societal costs and implications are profound.

Consumer protection harms

Consumer protection issues in online services include but extend beyond traditional privacy concerns:[87] Issues with fraud, scams, manipulation, discrimination, and systemic failures in content promotion and moderation have leveled devastating individual and collective harms.

A scale-at-any-cost growth mindset,[88] overly broad interpretations of intermediary liability laws that cover the sale of physical goods,[89] and other factors have disincentivized the development of more reasonable responsibility for consumer protection. For years, lawmakers have asked e-commerce sites to stop selling unsafe, banned, fraudulent, or knock-off products and asked other websites to stop advertising them.[90] A lack of quality control makes it easy to place false listings or reviews online to scam consumers, scam businesses, damage competitors, harass victims, and divert traffic from legitimate small businesses.[91] Negligent safety standards on large platforms have enabled bad actors to commit elaborate frauds, ranging from digital advertising schemes that scam advertisers to fake accommodations listings that defraud would-be guests to marketplaces that fail to protect users from scammers at scale.[92] In some cases, the gap between self-defined platform terms and actual enforcement across these issues is apparent.[93]

Due in part to the shift to online services during the pandemic, people are facing growing threats from long-standing consumer protection and cybersecurity issues. Losses to identify fraud, for example, topped $56 billion in 2020.[94] These costs are disproportionately felt: One analysis found that "Black people, Indigenous people, and People of Color (BIPOC) are more likely to have their identities stolen than White people (21 percent compared to 15 percent), and BIPOC people are the least likely to avoid any financial impact due to cybercrime (47 percent compared to 59 percent of all respondents)."[95]

Beyond sensitive financial and identity issues, the unprecedented amount of detailed behavioral data held by online services firms also poses unique consumer protection challenges. Platforms are able to exploit behavioral shortcomings and biases among consumers in real time to a greater degree than previously feasible.[96] They may intentionally complicate the process of changing privacy settings, opting out of data collection, deleting accounts, canceling services, and more.[97] These designs may hide or misrepresent costs,[98] fee structures,[99] and data collection.[100] In a digital environment, firms are able to more fully manipulate the buyer experience, making consumer manipulation of heightened concern.[101] Some firms employ deceptive behavioral design, sometimes called "dark patterns,"

which have been found to successfully manipulate consumers into giving up time, money, or information.[102] The ability to use detailed data and pricing systems has given rise to new forms of dynamic pricing, which too often replicate long-standing biases against historically marginalized communities.[103] Nearly three-quarters of Americans think this type of personal data-driven dynamic pricing is a "major or moderate problem."[104]

Online services have also given abusers and harassers more ways to locate and target victims while regularly failing to provide people with sufficient tools for preventing, curbing, or avoiding those attacks.[105] A recent poll found, "Of the types of harms people experience online, Americans most frequently cite being called offensive names (44 percent). More than 1 in 3 (35 percent) say someone has tried to purposefully embarrass them online, 18 percent have been physically threatened, and 15 percent have been sexually harassed."[106] Numerous online service companies have failed to take adequate steps to prevent these harms from occurring.[107] Over the past two years, the number of teenagers who reported encountering racist or homophobic material online almost doubled.[108] Marginalized communities—especially transgender people, immigrants, people of faith, people of color, and women of color—are disproportionately harmed through negligent or actively harmful platform business models around content and bear the brunt of their collective costs.[109]

Civil rights harms

Online services regularly introduce risks to Americans' civil rights and liberties.[110] Use of digital technologies—including software, algorithmic decision-making systems, digital advertising tools, surveillance tools, wearable technology, biometric technology, and more—have introduced new vectors to continue the deeply rooted historical exploitation of and discrimination against protected classes. Because privacy rights are also civil rights, these harms are inextricably linked to the privacy harms described above, wherein mined data feed into algorithms that are used to profile individuals, make decisions, target ads and content, and ultimately lead to discrimination.[111]

Leading scholars and advocates have exposed the numerous risks that automated decision-making systems—encompassing everything from static algorithms to machine learning to AI programs—pose to civil and human rights.[112] These systems can produce deeply inequitable outcomes, including and beyond issues of algorithmic bias.[113] Discrimination can occur at any point in the development process or produce, obfuscate, and launder discriminatory use.

Already, they have resulted in a slew of civil rights violations that materially affect Americans' liberty, opportunity, and prospects. Algorithmic decision-making systems have produced and reproduced discrimination in recruiting,[114] employment,[115] finance,[116] credit,[117] housing,[118] K-12 and higher education,[119] policing,[120] probation,[121] and health care,[122] as well as the promotion of services through digital advertising[123] and beyond.[124] Algorithmic racism in particular extends the project of white supremacy in pernicious ways:[125] With a glut of consumer data and the veneer of technical objectivity, online services companies have myriad ways to discriminate among consumers and obfuscate that discrimination.[126] For instance, digital advertisers can use proxy metrics to enable discrimination in advertising without technically using protected classes,[127] although Facebook has been sued for allowing discrimination based on protected classes explicitly.[128] Insurance, credit, and financial companies can bake historical data, which reflect long-standing inequities and biases, into decision-making algorithms that enable them to reproduce systemic racism and other biases while using a seemingly "objective" algorithm that processes applications in an identical manner—churning out preferential products and opportunities for white, wealthy people as they have for decades.[129]

Technology-enabled discrimination is especially dangerous because the application of these tools can be hidden and nonconsensual, limited forms of redress exist, and technical processes are often wrongly assumed to be objective, thereby receiving inappropriate deference or insufficient scrutiny. New AI and algorithmic hiring tools, for example, have been hailed for their "efficiencies," yet are found to compound existing issues in disability-based discrimination, despite long-standing Americans with Disabilities Act protections.[130] A range of algorithmic and platform design choices can likewise enable discrimination.[131]

Facial recognition and other biometric surveillance technologies erode civil liberties, particularly for communities of color.[132] The biases in these technologies[133] and their use by law enforcement[134] have led to traumatic violations of civil liberties, including a number of recent wrongful arrests of innocent Americans who were misidentified by faulty facial recognition software.[135] But more broadly, their increasing use in public spaces and employment as tools to continue the overpolicing and oversurveillance of people of color threatens civil liberties, chills political speech, and inhibits freedom of movement and assembly.

Content moderation challenges and negligence also introduce asymmetric risks to protected classes. Platforms' failures to prevent the exploitation of social networking for purposes of harassment, discrimination, hate speech, voter suppression,

and racialized disinformation have made long-standing problems newly urgent. Furthermore, major platforms have been found to increase radicalization and participation in extremist groups.[136] At the individual level, these problems have subjected people to harm and serious duress[137] and enabled the deprivation of rights, including the right to vote.[138] Civil rights experts have drawn parallels between the discriminatory nature of these business decisions and platform designs and the public accommodation laws that protect against discriminatory practices in brick-and-mortar businesses, highlighting the need to update and reinforce current digital protections.[139]

Collectively, the sheer quantity and amplification of such civil rights-suppressing content introduces barriers to and discourages full participation in public life and cultural discourse by already excluded groups. The prevalence of false information and propaganda on social media in particular can grossly warp public discourse and societal understanding of public events. Misinformation has been used to maintain and advance racist, sexist, transphobic, and other prejudices, while "astroturfing" strategies—wherein coordinated networks of accounts, including "fake" accounts not representing "real" people, artificially inflate the popularity and visibility of certain posts—are used to misrepresent the prevalence of these attitudes. For example, despite the majority of Americans supporting Black Lives Matter, 70 percent of Facebook posts from users discussing the topic in June 2020 were critical of the movement.[140]

Beyond posing risks to specific enumerated rights and liberties for protected classes, online services have reified, maintained, and extended racism, sexism, and other social prejudices generally in the United States, through both their technology development and business model negligence. For example, Dr. Safiya Noble's pioneering work illustrated that, for years, searching "black girls" on Google returned pornographic search results and ads, whereas searches for "white girls" did not.[141] Similarly, searches of Black-identifying names disproportionately returned ads mentioning "arrests" compared with searches of white-identifying names.[142] Numerous other instances of search engine and predictive text results enhancing and extending social discrimination abound,[143] and similar problems exist in voice technologies, facial recognition, and other biometric and visual processing techniques.[144]

Across these four overlapping and interconnected areas of harm—economic, privacy, consumer protection, and civil rights—the information asymmetry and power of online services firms threaten to impede understanding and responsible regulatory solutions. Specifically, massive spending power and political leverage

strongly influence regulatory and political environments, as well as firms' ability to shape media and public discourse in their favor. Finally, as noted above, the lack of transparency regarding economic activity, data collection, and content moderation makes it difficult to identify or verify suspected harms.

Finally, Americans have long recognized the unique political power of media industries and the importance of pluralism and diversity in the press. Every major emergent communications technology in modern history, from the printing press to television, has engendered new challenges and problems.[145] However, Americans are especially concerned about the power online services have over public discourse and the political system. Recent surveys show that approximately 81 percent of U.S. adults, and majorities of voters of both political parties, believe that technology and social media companies "have too much power and influence in politics."[146] Likewise, 77 percent of American adults believe it is a major problem that online search and social media platforms control what people see on their platforms. Simply put, concentrated power in online services—particularly among social media, search engines, and cloud infrastructure—are cause for democratic concern and action.

Regulatory gaps in addressing online harms

Existing laws, authorities, and agencies can address a subset of interlocking online services harms outlined above. In particular, the Center for American Progress strongly supports more aggressive antitrust action,[147] more robust competition policies,[148] increased privacy and civil rights capacity at the FTC,[149] and strong federal privacy legislation or rules.[150] The 117th Congress has an opportunity to achieve key gains in these areas by passing the tech antitrust package—which has been reported favorably out of the House Judiciary Committee[151] and for which companion bills have been introduced in the Senate[152]—fully resourcing the DOJ and FTC,[153] and settling on a strong federal privacy proposal. Significant progress is on the table.

Looking ahead, however, even an optimistic reading of these proposed updates shows gaps would persist in the government's ability to tackle the vast scope of online services harms in a timely and effective manner. As outlined below, existing systems of regulatory oversight are primarily reactive: Judicial scrutiny and dedicated, but often narrower, piecemeal legislation have struggled to keep pace with technological and market change. In a vacuum of regulatory scrutiny, consumer harms have accumulated, predatory practices have become industry standards, and dominant players have entrenched and expanded their holdings. Over time, a regulatory "debt" has built up where existing statutes and sector-specific regulations have not been sufficiently updated or applied to novel problems. Labor laws, for example, have lagged behind developments in algorithmic workplace management systems. Effective regulatory oversight must grapple with not only emerging issues but also the regulatory debt that has developed over past decades.

Historically, developing remedies has taken years, sometimes more than a decade, to reach resolution after harm has occurred. While it is certainly possible for congressional oversight to dedicate the required expertise to online services regulation—as seen in the historic 2020 House antitrust report[154] and resulting bipartisan legislative proposals from the House and Senate in the 117th Congress—it is impractical for them to do so for dozens of different online services industries presenting novel problems, or old problems in new bottles. This is particularly true for small

and medium-sized players that require regulation but lack the public recognition or political attention merited by digital gatekeepers. Significant federal investment in public interest oversight and administrative bodies is needed to understand and rectify the problems that have proliferated during the past 20 years.

Basic regulatory capacity has not kept pace with the growth of online services. This section surveys current regulatory tools and identifies the outstanding gaps. It presents a mix of current gaps and those that would likely remain if privacy and competition developments are enacted.

Gaps in addressing economic harms

Economic harms could be partially addressed through existing antitrust laws, including the Sherman Antitrust Act and Clayton Antitrust Act,[155] as enforced by the U.S. Department of Justice (DOJ), FTC, and state attorneys general.

However, over recent decades, a successful movement to narrow the application of antitrust laws to a limited consumer welfare standard has allowed monopolies to flourish across industries. The anemic antitrust enforcement that has resulted has enabled increased concentration of power in many sectors, including technology and online services markets.[156] Existing authorities are limited in their abilities to increase competitive pressure on already dominant firms. Furthermore, limitations exist in addressing market dominance arising from inherent network effects; conventional antitrust does not necessarily forbid monopoly in the absence of exclusionary, improper, or predatory acts. Where applicable, antitrust tools can be slow: With important exceptions, such as merger reviews, many are limited to after-the-fact intervention. These qualities have hampered antitrust effectiveness in the online services space, where remedies are sometimes pursued too late.

Revived enforcement is essential to remedying current problems and promoting competition.[157] Recent actions from U.S. enforcement agencies—such as the antitrust suits filed by the FTC, DOJ, and state attorneys general against Google and Facebook, as well as other ongoing investigations—are positive steps toward these goals.[158] These cases use existing authorities to address economic harms including negative impacts on innovation, pricing, and labor.

Unfortunately, complex court cases have yearslong timelines. The outcomes of these cases are uncertain—and even more so due to the difficulties in applying a deficient consumer welfare standard to digital markets. The conservative shift in

the federal judiciary over past decades and the high bar set by existing antitrust laws and court decisions further complicate enforcement. Even in the event of a successful case, the ensuing appeals process may take years, and selected remedies may fall short of those that would most effectively address anticompetitive effects, such as structural separation, reversal of mergers, or divestiture.

During the years it takes for cases to work through the courts, tech giants will continue to expand, entrench, and potentially abuse their dominance. Monopolists under scrutiny may well outlast any viable competitors and the government administrations that bring suits to challenge them in the first place. Injunctive relief during investigations may help prevent further consolidation but is only a temporary, limited measure. Some experts have argued that the threat of potential antitrust action makes dominant companies operate more cautiously and accept competitive measures that they would otherwise oppose. However, companies often calculate the bare minimum required[159] to escape with their dominant market share intact;[160] given the scope, scale, and importance of online services to the United States, self-regulation and deterrence are no longer viable strategies.

Beyond revived antitrust action, a number of complementary competition policy reforms are needed.[161] These include increasing the focus on anticompetitive conduct by dominant firms, making antitrust enforcement more transparent and robust, and setting out clear new rules against self-preferencing or discrimination by dominant platforms.[162] In 2020, the House Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law issued a landmark report on digital markets and gatekeepers, illuminating a number of the anticompetitive issues in digital markets.[163] In 2021, the House Judiciary Committee reported favorably out of committee a suite of new antitrust and competition policy bills designed to address these issues.[164] For covered online platforms, the bill introduce pro-competitive provisions around nondiscrimination and self-preferencing,[165] mergers and acquisitions of competitors,[166] interoperability,[167] merger filing fees,[168] lowering barriers to state antitrust enforcement,[169] and eliminating fundamental conflicts of interests between platform operators who wish to compete within their own marketplace.[170] The American Innovation and Choice Online Act would also call for the creation of a new Bureau of Digital Markets within the FTC to handle the increased workload and specialization that digital markets require.[171] These proposals, and the Senate companion bills,[172] offer a powerful opportunity to address some of the most pernicious anti-competitive practices used by online services gatekeepers today. Looking to the future, additional work will be needed as new markets, predatory practices, and gatekeepers emerge—including and beyond those that would currently be covered under the bills' proposed tests.

Gaps in addressing consumer protection harms

A patchwork of state and federal laws target consumer protection issues posed by online services, from the Better Online Ticket Sales Act,[173] to the Children's Online Privacy Protection Act,[174] to the Restore Online Shoppers' Confidence Act,[175] among others. Broadly, however, the FTC is charged with protecting consumers by stopping unfair, deceptive, and fraudulent practices—which includes practices employed by online services providers.[176] The FTC is generally the primary agency addressing consumer protection issues from online services, though other agencies such as the Consumer Product Safety Commission and Consumer Financial Protection Bureau (CFPB) may play a role depending on the specific sector or focus of a company. State attorneys general also have consumer protection responsibilities, although many states have weak or ineffective unfair and deceptive practices laws.[177]

On a federal level, years of aggressive opposition have limited consumer protection and the FTC's ability to effectively enforce them. Scaled-back use of FTC rule-making in recent years has likewise contributed to growing deficiencies in consumer protection online. Some observers, including former FTC commissioner and current CFPB Director Rohit Chopra, have argued that the agency has been shy about using the full range of existing authorities.[178] Others have suggested that it is "overburdened" with an immense jurisdiction and limited resources, pointing to a history of companies requesting to be placed under FTC oversight in order to "get its issues lost amid the issues of other companies."[179]

Despite its broad consumer protection and competition mandates, the FTC is not a large agency. It fulfills its mission with limited capacity: about 1,160 full-time employees to cover consumer protection in most sectors. This number has dropped significantly over the past several decades. Consumer Reports recently noted that, since 1979, "the economy has grown nearly three times while the FTC's capacity has decreased 37 percent."[180] The FTC Office of Technology Research and Investigation has only a handful of staffers to support work across the agency.[181]

Enhanced consumer protection regulation and new legislation are required to protect Americans online. Given the scale and variety of consumer protection harms from online services, existing FTC authorities and capacity are manifestly insufficient. However, as noted below, recent developments are a promising start to restoring and elevating the agency to the capacity and authority needed to fulfill its mission.

Gaps in addressing privacy harms

The United States is unique among its peers in that it still does have a national data privacy law. Consequently, it also lacks a designated data protection agency. In lieu of such a body, the FTC serves as the de facto data privacy agency: Its authority over unfair and deceptive acts or practices has been brought to bear against online privacy and security violations,[182] and it serves as the regulator for the 1998 Children's Online Privacy Protection Act. As FTC Commissioner Rebecca Kelly Slaughter noted in 2020, however, "In enforcing data privacy, the Commission does not have the most straightforward tools. The FTC has done an impressive job of attempting to curb the worst abuses in this space without the benefit of a federal privacy law, civil penalty authority, or anywhere near the dollars or the bodies that other countries devote to data privacy protection."[183] Indeed, the FTC has only 40 employees focused on data protection.[184] By comparison, the Irish Data Protection Commission, the primary EU regulator for many large U.S. tech platforms, is only one of the EU's 31 data protection supervisors[185] and has three times as many staffers.[186] It still faces regular criticism for its slow pace and large workload.[187]

Absent comprehensive federal protections, states have also increasingly adopted privacy protections through legislation or statewide referendums, starting with California in 2018 and 2020[188] and Virginia and Colorado in 2021.[189] Given California's influential status as a population center and the home base to many technology companies, its state laws have unique nationalizing effects in the absence of federal law—for example, the 2003 California Online Privacy Protection Act was the first state law to require privacy policies to be posted on a website.[190]

Thus far, the limited powers of existing regulatory agencies have not sufficiently protected and empowered Americans in the current data environment.[191] For example, a recent New America Open Technology Institute report noted:

> *The FTC's approach primarily relies on corporate self-regulation under the notice and consent model, bringing enforcement actions against companies that have deceptively violated their own privacy policies and public representations made to users about how they protect their privacy and security. While this strategy has led to a number of enforcement actions over the years, the notice and consent model relies on a number of faulty assumptions, including the notion that the average user can meaningfully consent to privacy policies.*[192]

However, as outlined in a recent report by the Electronic Privacy Information Center,[193] the FTC does have unused authorities it could exercise around online privacy. Commissioners have shown recent interest in reviving the FTC's latent authorities to tackle data privacy, including the Magnuson-Moss Warranty Act rule-making authority.[194] Under new leadership, there are indications that the FTC may move to make better use of these authorities,[195] including over privacy harms.[196] And given the pressing need for consumer protection online, lawmakers have recently proposed increasing funding to the FTC to expand its privacy focus.[197] As noted above, these efforts must overcome the FTC's capacity constraints, limitations to its traditional rule-making ability, and reliance on consent decrees—which have become increasingly routine and symbolic for corporate America. Privacy must also compete with other issues at the FTC, whose limited capacity requires picking and choosing issues within its broad mandate.

Complementary to any renewed privacy efforts at the FTC, strong federal privacy legislation is necessary and overdue. Fundamentally predatory data collection practices must be prohibited. The federal government must establish increased enforcement capacity to guard against the numerous harms of nonconsensual data collection, sale, and discriminatory use. Federal legislation should include robust civil rights protections, strict limits on the use of personal data, limitations on consent-based models, enhanced individual rights and privileges, and action paths to defend new rights for individuals and state governments. Recognizing a critical need for increased capacity, federal privacy proposals from both Republicans and Democrats include giving the FTC increased rule-making authority over privacy,[198] and Sen. Kirsten Gillibrand (D-NY) has proposed creating a new data protection agency.[199] As part of a new social spending package, the U.S. House of Representatives also proposed significant investments in the FTC to create a new privacy bureau.[200]

These steps would provide a badly needed foundation for guarding Americans' privacy. A new privacy law, however, may not be able to address new and creative abusive behaviors that will inevitably arise. Few proposals would holistically grapple with the chilling effects of pervasive, ambient personal and biometric surveillance. The practice of surveillance advertising[201] may be difficult to curb so long as the incentives stay in place and the behavior remains legal. Finally, privacy is not the sole lens through which to judge the impact of online services; tensions must be dynamically balanced among privacy, security, competition, transparency, and other priorities.

Americans across the political spectrum are strongly in favor of robust federal privacy protections,[202] and in order to properly enforce those restrictions, regulatory bodies need additional administrative rules and capacity along those lines. Here, as with competition and antitrust approaches, new statutes, enhanced capacity, and specialist oversight are required to effectively govern online services.

Gaps in addressing civil rights harms

The evolution of online services has outpaced the application and interpretation of civil rights laws to digital properties and transactions. In general, civil rights laws apply broadly, including to online behavior, transactions, and properties; the law, for example, does not distinguish between discrimination in employment advertisements in a newspaper and online. Yet in practice, the protection of civil rights online has lagged behind emerging and present risks, outpacing the ability of the DOJ, Equal Employment Opportunity Commission, U.S. Department of Health and Human Services, U.S. Department of Agriculture, and other federal and state enforcement bodies and officers to identify and investigate potential violations. Numerous groups, including the Center for American Progress, have called for the creation of an Office of Civil Rights at the FTC to strengthen its ability to prevent discrimination and protect equal opportunity online.[203]

However, beyond capacity, some argue that a lack of clear case law or uncertainty around what case law is applicable to novel technologies can impede enforcement efforts. Where relevant case law does exist, application of the existing doctrine to online services discrimination cases is not always straightforward.[204] Significant work is required to grapple with the substantive challenges posed in some, though certainly not all, online or data-driven discrimination cases where the structures or business systems involved in the online service provision do not map neatly onto existing templates in case law. Once again, the numerous barriers that exist in algorithmic accountability and transparency[205] have further complicated effective civil rights enforcement.[206]

While in most cases there is no question that existing civil rights laws apply online, any approach to regulating online services should forcefully reject certain questions about how existing laws apply, ensure that there is effective and robust enforcement of these laws online, and close any loopholes that may exist for narrow "frontier" areas where existing laws may not have predicted harms. Given the sheer scope of the new transactions, interactions, and digital properties involved in the provision of online services, significant, proactive work can ensure that Americans' civil rights are protected and prioritized.

Illustration of outstanding gaps: The question of Facebook and Instagram

Consider the application of existing tools to the case of Facebook, Inc. (The company recently changed its corporate name to Meta Platforms, Inc., but for the purposes of this paper, will continue to be referred to as Facebook.[207]) Facebook appears to have acted anti-competitively.[208] In 2021, the antitrust case brought by the FTC against Facebook[209] was dismissed by a federal judge[210] and refiled by the agency.[211] If the case is successful and the FTC is granted all requested remedies—including rolling back Facebook's acquisitions of WhatsApp and Instagram—the divestitures would remedy ground gained anti-competitively. But they would only go so far in preventing abuse of consumers on Facebook's main platform, Facebook Blue: the largest social network in the world.[212] Moreover, Instagram would be in a position to copy Facebook's problematic practices around privacy, discrimination, competition, and general lack of accountability for design choices and business decisions. Breaking up a predatory company may reduce the scale of harm and introduce new competitive incentives, but it does not necessarily prevent continued predatory practices—described by Harold Feld as a "starfish problem."[213] Alternatively, the proposed tech antitrust bills would address a range of issues—including ending self-preferencing, encouraging interoperability, and instituting a higher bar for future efforts to acquire nascent competitors. However, since the newly independent Instagram would likely not meet the bill's requirements for a covered platform, it would not, unlike Facebook, be subject to the new competition policies—even if some of these practices should arguably not be allowed at all. Indeed, new data portability might allow Instagram to implement a nearly identical version of Facebook's targeting algorithms—likely faster than other competitors due to familiarity and existing technical architecture—allowing it to crush new entrants. A new federal privacy law may return greater control to users in managing the huge amount of data that Facebook and Instagram have collected on them but would still allow for much of the first-party ad targeting that brings in a majority of the platforms' revenue. Similarly, outright banning of targeted advertising would leave a significant advantage to Facebook, which is in a prime position to pivot to contextual advertising through its first-party properties.[214] Finally, while Facebook has previously settled lawsuits around discriminatory advertising, the public will still have few assurances that the company or divested businesses do not continue to harm civil rights.[215] Aggressive antitrust action and structural remedies, new competition laws, and new privacy laws are all clearly needed, but would still leave gaps that allow for consumer, competitive, and civil rights abuses perpetrated by Facebook and Instagram.

A new regulatory model to address gaps

Even in best-case scenarios for critical competition and privacy updates, significant gaps would remain in the U.S. government's ability to anticipate and remedy online services harms. To effectively govern online services, U.S. regulators need to be empowered with proactive rule-making abilities that can curb problems before or as they occur. Such proactive rule-making powers—sometimes called "ex ante" regulation—are distinct from reactive or "ex post" approaches, which are litigated after harms have occurred. Proactive rule-making could identify and prohibit harmful measures prior to significant harm or as harms are occurring.[216] In other words, this report proposes complementing after-the-fact antitrust enforcement by adding new restrictions and regulations that help prevent harm across multiple areas.

Regulatory tools go hand in hand with antitrust enforcement, which is the government's best vehicle to address persistent anti-competitive behavior by individual companies. But, as noted above, antitrust tools are not necessarily well-matched to the range of noncompetitive harms posed by online services of all sizes. Yearslong timelines and uncertain outcomes further underscore the need for a parallel regulatory process. Going forward, adding new oversight powers could more quickly surface or address problems that require antitrust action. A center of excellence within the executive branch could expand the courts' enforcement and oversight options when determining appropriate remedies. As FTC Commissioner Rebecca Kelly Slaughter testified before Congress in March 2021, "Effective enforcement is a complement, not an alternative, to thoughtful regulation. That is especially true for regulatory models that cannot be effectuated by ex post enforcement actions, even those with the broadest deterrent effect."[217]

Increased regulatory oversight of online services can be a sensible complement to existing sector-specific regulations. In taking a cross-cutting approach, regulators could address the common aspects of problems that are unique to the online nature of service provision without necessarily affecting the many different industry-specific rules developed to govern the underlying services themselves. This is particularly true for sector-specific regulations in transportation, finance, labor, and other areas where there may be overlap. In *The Case for the Digital Platform Act*,

Harold Feld writes that much like the pharmacy within a grocery store is regulated without subjecting the entire grocery store to pharmacy constraints, the online services offered by that grocery store can have dedicated regulation without necessarily subjecting its various other business practices to identical rules.[218] Consider also, for example, how the U.S. Food and Drug Administration regulates prescription medication production very differently than it does growing vegetables—and within that, regulates industrial-scale vegetable production with some precision but stays out of home gardening. In the same way, dedicated online services regulation can scale by risk level and industrial heft where needed, rather than subjecting major e-commerce platforms and hobby webhosts to identical rules.

To be clear, while the proposals here are designed for online services, they are not all designed to apply to every online service; rather, online services are the universe in which common problems arise, and the rules proposed here would enable regulators to target specific problems within that universe.

This report advances a three-part regulatory framework for online services. It groups the two most distinct subsets—infrastructural services and dominant gatekeepers—apart from online services more generally. Services can opt in to online infrastructure regulations, subject to certain restrictions, qualifications, and regulator approval. The services that do not self-select as online infrastructure will fall into the general online services tier, regardless of their size. Those qualifying as gatekeepers will face additional, targeted regulations beyond the general online services regulations. The following sections sketch the parameters of each tier, noting target services, proposed regulation, and interactions with other tiers.

Online infrastructure services

Online services provide essential infrastructure for the American economy, culture, and society. Cloud infrastructure, content delivery networks (CDNs), web hosts, and data analytics services are the quiet but dynamic backbone of the commercial internet. These online services now act as infrastructural components to other economic and social activity. They are generally lower on the stack than the more consumer-facing services at the top of the stack. (For more on the conceptual model of the internet stack, see Figure 1.) They are constant and ubiquitous, even if invisible to most internet users, and for this reason are often overlooked by regulators and the public until something goes wrong.[219] A special focus on online infrastructural services is warranted due to their tremendous impact on the economy, the environment, cybersecurity, human rights, and freedom of expression.

To preserve, secure, and strengthen online infrastructure, this report proposes a mix of public interest obligations—such as common carriage, interoperability, security, and environmental protections—with dedicated intermediary liability protections independent of those under Section 230. The proposal targets largely unregulated online infrastructural services that are higher up the stack from FCC control of internet service providers at what are sometimes called "edge providers."[220] This approach adopts what scholar Annemarie Bridy describes as "layer-conscious internet regulation,"[221] and adds to the discussion a distinction between infrastructural and other providers *within* the application layer, not just between the application and network layers.

For now, this proposal stops short of suggesting that these services be treated as public utilities. There are myriad examples of common carriage principles being applied to services that are neither public utilities nor regulated monopolies. The authors' intention is that no lawful actor wishing to pay the established rate for online infrastructural services shall be denied or otherwise discriminated against so long as they are not publishing illegal content.

The rationale for this proposed mix of obligations and protections is threefold: (1) discriminatory pricing practices can stifle innovation and competition; (2) infrastructural digital services pose different regulatory problems than the consumer-facing websites, services, and apps they support; and (3) there is substantial risk to freedom of expression when content regulation is pushed lower on the stack.

First, equal access to infrastructural services is foundational to ensuring free and fair competition across all online services that depend on them. In cases where these services are provided by companies offering other online services, there may be strong business incentives to opaquely employ differential pricing or restrictions in access. Additionally, this is a market where companies have erected significant and asymmetric barriers to customer entry and customer exit—for example, by levying much higher costs to transfer data out of a service than to import it.[222]

Second, the business decisions of online infrastructure have outsize effects on the security, accessibility, and resiliency of online services. They also have a significant material impact on energy consumption and the physical environment.[223] Towns in which data centers are located face difficult choices around dedicating the water and electricity resources required to support them; a typical data center uses as much water per day as a small city, and many are located in arid,

drought-plagued regions of the country.[224] And while infrastructural services have been designed for performance, security, and reliability, they are generally not structured to offer the transparency and due process provisions that responsible content management requires. Forcing greater public visibility and monitoring systems into these services may adversely affect efficient, secure transmission of internet services to businesses and consumers. Taken together, this presents a strong argument for pushing content regulation to the edges—where consumer-facing services can more reasonably be expected to perform rights-respecting content moderation[225]—while also developing dedicated regulation for the security, environmental, and other aspects that are specific to online infrastructure.

Third, decisions by online infrastructural services have powerful effects on freedom of expression.[226] Lacking due process, transparency, or accountability, infrastructure-level moderation offers blunt choices that, as Jack Balkin notes, may have significant collateral effects.[227] Restrictions on arbitrary content-based discrimination by infrastructural providers could offer important provisions for freedom of expression, particularly for groups that are at risk of facing systemic discrimination.[228] And while recent content moderation battles have involved infrastructural services—such as Amazon Web Services removing Parler after the January 6 insurrection[229]—the risks posed by inappropriate moderation among infrastructural services are high and may generally outweigh the benefits gained by enabling continued discretion for the reasons outlined above. Both deeper empirical study and a broader normative conversation about these choices are necessary, but such a choice would favor equitable service provision over maintaining the ability for providers to discriminate, even against heinous but lawful content.

Online infrastructure services were developed under the intermediary liability protections of Section 230 of the Communications Decency Act, which allows online services and internet users to provide and moderate content from others without being held liable for third-party content or their good faith moderation decisions.[230] Recently, Section 230 has been targeted for reform by liberals seeking to combat disinformation on social media platforms and by conservatives for alleged censorship or suppression of conservative voices on those same platforms.[231] Some of these proposals have been well-tailored to particular areas of concern, while others have been disconnected from the actual changes they might precipitate. In either case, significantly changing Section 230 protections in response to problems in the consumer-facing application layer may result in significant negative disruptions to many online services and likely have unintended consequences for infrastructural services. Reform or repeal of Section 230 would powerfully affect the speech of individual users—particularly those from traditionally marginalized groups—not just on gatekeeper platforms, but also across

every website, app, and backend service. CDNs, cloud hosts, and other infrastructure providers may face the reality that their business models are no longer viable due to liability issues. Few proposing reform or elimination of Section 230 wish to unintentionally incapacitate such a wide array of everyday services, which is why recent proposals are increasingly exempting infrastructural players.[232]

Thus, the federal government must simultaneously enhance areas of responsibility for online infrastructure services and implement protections to ensure that these services are not unintentionally upended by any potential intermediary liability changes. Taking lessons from the benefits and challenges that have emerged over the years around Section 230, the public interest requires a mix of protections and obligations that are appropriate specifically for infrastructural services.

Target services

Online infrastructure has changed significantly over the past 20 years and continues to evolve. Today, the current crop of cloud technologies allows for numerous backend infrastructure tools—such as remote storage, raw computing, and proprietary software accessed remotely—to be offered as on-demand services that power everything from small-business websites to the largest online platforms. Although recent trends have been toward concentration and centralization of the cloud, the push for data localization and rise of 5G connectivity, edge computing, and blockchain suggest the possibility of more decentralized infrastructural services. Regardless, the demand for computing power continues to grow, and expectations of instantaneous and global access will drive continued evolution in infrastructure technologies.

In light of these crosswinds, drawing a precise, static line in the stack for which online services should be considered infrastructure is challenging[233] and may only grow more difficult. To ensure that this model encompasses the companies and products whose goal is to operate as infrastructure, without unnecessarily impeding innovation or market evolution, this proposal would allow businesses to self-select and opt in a business line to the new regulatory model, subject to meeting designated structural requirements and approval by the regulating entity.

An opt-in approach offers a degree of future-proofing that may be difficult to provide through statutory definition alone. Allowing companies to generally opt in ensures that only those that consider themselves infrastructural and understand the requirements choose this model; this is expected to comprise a minority of online services overall. This approach may enable new companies to start

with the explicit goal of competing as online infrastructure and would offer all infrastructural companies a strong defense against the technical, legal, and public relations costs resulting from good and bad faith demands for increased content moderation lower in the stack. While challenges exist around the incentives and consequences for infrastructure providers in and outside of the tier, those opting in would be regulated by an entity that prioritizes the goals of online infrastructure. Infrastructural firms outside the tier will have to deal with rules designed for broader online services or gatekeepers and deal with the business realities of any potential intermediary liability changes. Business customers will be able to exercise choice in determining which online service provider may best meet their infrastructural needs.

Even with an opt-in approach, regulators will need criteria for eligibility to help clearly describe the target audience and guide them in preventing abuse. Given the variety of service architectures in this space, flexible criteria are key. Administrators of the online infrastructure rules, in conjunction with technology experts at the National Institute of Standards and Technology (NIST), should be tasked with helping to assess qualifying online infrastructure services and developing such criteria. Some, but not necessarily all, of those characteristics of online infrastructure could include:

- Primarily nonconsumer-facing for configuration, storage, presentation, and delivery of online content
- Primarily paid services used on the backend to provide broader platforms or services to consumers or commerce
- Designed to ensure the fulfillment and delivery of other services
- Existence of the service is materially important and enables continued full participation online of other entities and individuals

This report does not envision that payment processors or decentralized payment platforms would be eligible to opt in to the online infrastructure class in its initial establishment. Financial transactions are too enmeshed in the existing financial regulatory system, fraught with broader policy implications that require deeper consideration outside the scope of this report.

The business lines that opt in to the online infrastructure tier would not be subject to the general online services and gatekeeper regulations described later in this report, although select rules may be mirrored from those tiers. Notably, there is a strong incentive for companies to opt covered business lines in to the dedicated online infrastructure regime. If they do not do so, and have been designated as a

gatekeeper, an infrastructural business line would be fully subject to gatekeeper regulation in addition to general online services regulation; alternatively, that business line, if sufficiently dominant, could qualify the entire company as a gatekeeper.

Companies with existing online infrastructure business lines, including those run by entities that will be designated as gatekeepers, will need to undergo a specific process to bring that business line into the opt-in online infrastructure model. First, companies would need to engage in a series of steps to separate the data and operations of the designated online infrastructure product from their other lines of business. In some cases, the easiest way to do this may be to establish an entirely new, separate entity. Such an approach is not without precedent. For example, the National Bank Act allows banks only to engage in certain prescribed activities; if a bank wants to engage in nonbanking activities, it has to create a holding company and create affiliates to do the nonbanking work. Importantly, any interaction between the bank and nonbank entity would need to be an arms-length transaction, as if they were doing business with an unaffiliated firm. Similar restrictions could apply here.

Second, strict data confidentiality restrictions for companies with business lines in multiple tiers will also be put in place. The entity would have to agree to these restrictions by attesting to them at the corporate and CEO level, with substantial civil and criminal penalties for the company and executives. Third, the regulators responsible for overseeing online infrastructure can veto an entity that they believe has not met the requirements and potentially even conduct a renewal process periodically to ensure appropriate inclusion. Finally, if an entity that has previously opted in to the online infrastructure class wished to exit that tier, there would be a required exit period of at least three years, and the company would be regulated as a general online service upon exit and assessed for potential gatekeeper qualification.

While business lines in the opt-in online infrastructure tier would not be eligible for gatekeeper status, in the tradition of infrastructural regulation, there may be individual services or submarkets of online infrastructure that become so critical to the operation of online infrastructure that they mirror traditional essential or critical infrastructure. Therefore, an essential or critical infrastructure designation for certain services or submarkets should be explored in conjunction with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Administration and subject to additional requirements if so designated, with the specific goal of ensuring reliability, security, and access. Related strategies are already being explored around cloud systems in the financial services sector,

including the request of Reps. Katie Porter (D-CA) and Nydia Velázquez (D-NY) to the Financial Stability Oversight Council to designate cloud storage providers as systemically important financial market utilities.[234]

Proposed regulation

Inspired by the robust progressive tradition of protecting the public interest in critical parts of the economy, the foundational responsibilities imposed under this tier are common carriage and interoperability requirements to ensure fair treatment of competitors and adjacent services. This report focuses on two components of common carriage: access and nondiscrimination. Specifically for online infrastructure services such as web hosts, this will require both access to the service by any lawful entity for lawful content and nondiscriminatory pricing of the services; that is, different classes of hosting services may have different prices, but hosts cannot price discriminate among customers within those services. Hence, incorporation of common carriage requirements protects against both content and economic discrimination.

While the tenets of mandated common carriage and content nondiscrimination do not make sense for every online service, they are appropriate for online infrastructure. Whereas there are times where higher-stack, consumer-facing online services need to exercise greater discretion and assume greater responsibility for the activity enabled by their online business products, lower-stack infrastructural services generally need the opposite: protection from any increasing liability for the consumer-facing services they enable and requirements to deal equitably among legal content and customers.

For online infrastructural services, common carriage and greater intermediary liability protections should go hand in hand. This would eliminate the ability for infrastructure providers to arbitrarily discriminate among their customers, compel them to carry all legal content, and insulate them from inappropriate legal liability or evolving changes in liability for their service provision. Legal content does not mean all content. Content that violates federal law such as child sexual abusive material,[235] accounts from designated foreign terrorist organizations,[236] or content in violation of sanctions programs or from sanctioned countries[237] would continue to be prohibited and require legally appropriate preventative measures. In extremely narrow cases, Congress could allow the regulator to identify other specific exemptions.

The tradition of common carriage in the telecommunications space also provides useful references for conceptualizing appropriate public safety obligations. Telecommunication providers are required to facilitate emergency services such as 911 connections and emergency information. In a similar vein, services opting in to the online infrastructure model could be required to provide certain standardized public safety measures. These could include clear requirements and standards on reporting illegal content, such as incitement to violence, time and process requirements for the service to investigate and act, referral requirements to appropriate law enforcement entities, and standard lawful preservation requests.

The goal of the online infrastructure class is to ensure the continued fulfillment and delivery of online services. This does not just mean technical rules around ensuring stability or security but ensuring that customers have broad ability to prevent legal, pricing, or technical lock-in. For example, an online infrastructure regulator could not only ensure clear price transparency and billing recourse but also prevent abusive contractual, technical, or economic lock-in costs.

Beyond the common carriage obligations addressed below, additional obligations imposed under online infrastructure's public interest bargain might include cybersecurity standards, privacy rules, and environmental standards, particularly given the significant and growing environmental impacts of data centers that are too often overlooked.[238]

For regulators, being able to craft more stable rules specific to strengthening and protecting online infrastructure should be easier than crafting broader rules for online services, and indeed should remove a roadblock to crafting appropriate regulations for consumer-facing services. Under the status quo, much of the legislation targeting online services—which is primarily conceived for consumer-facing rather than infrastructural services—would need to include infrastructure exemptions to target restrictions to have their intended effects. In contrast, the Center for American Progress proposes distinct tiers that disentangle fundamentally different roles in online services provision and should enable better regulation with fewer unintended consequences in both cases.

General online services

The speed, scale, and novelty of some online services markets have at times challenged regulators, but so has the deliberate obfuscation and misdirection by online service providers seeking to evade government oversight, sometimes relying on exaggerated claims of their own complexity or novelty to defend against regulation.

Industry speed and complexity, however, are not insurmountable challenges to restoring democratic oversight. The federal government needs to establish sufficient expertise to assess, communicate, and regulate, on behalf of the American public, the practices, technologies, benefits, and harms associated with online services. To anticipate and encourage innovation while protecting the public interest, significant regulatory enhancements and statutory protections are needed to protect consumers, safeguard civil rights, and promote competition online.

For general online services—all services outside of the online infrastructure tier proposed above—this section proposes to enhance the following tools and capabilities:

- **Oversight powers,** including investigative, disclosure, and assessment functions to systematically improve transparency and public understanding of online services.
- **Referral and collaboration powers,** to most effectively leverage existing statutes and support sector-specific regulators in promulgating updates where needed.
- **Lawful principles and rule-making powers,** structured around eight principles laid out by Congress, which form the basis of four lawful prohibitions for online services—anti-competitive practices, insecure and data-extractive practices; unfair, deceptive, or abusive acts or practices; and civil rights violations. Regulators would consider four important factors in promulgating specific rules based in Congress' general principles—equitable growth, innovation, representation of all participants, and information diversity and pluralism. Congress should similarly outline per se violations of these categories to outlaw highly problematic practices where they are already observed and understood, while being clear that this enumeration is not exhaustive and can be expanded by the regulator. These rules would be backed up by a wide range of appropriate enforcement powers.

In enforcing these rules, robust options should be put on the table: civil enforcement, criminal enforcement, fines, and criminal penalties for executives will all have a role to play in enforcing the general online services rules promulgated under the new model.

Oversight powers

A mandate for ongoing oversight, new investigatory responsibilities, and enhanced disclosure and transparency powers are an essential foundation for online services regulators. At present, the stark asymmetry in knowledge and data about online harms between online services companies and everyone else

means that regulators, academics, journalists, and the public are at a significant disadvantage in trying to understand even the broadest strokes of issues online. The ability to investigate, audit, and publish reports about online services markets and emerging issues, such as bias in machine-learning programs or the impact of algorithmic amplification on disinformation, would allow for significantly improved transparency and understanding. Specific obligations should be given to regulators to investigate emerging problems and problems for which online services regulators may be the sole oversight body.

Research and investigatory authorities would need to be sufficiently broad to encompass products, features, algorithms, business practices, or other technical architectures of online services. Specialist regulators could produce new reports or impact assessments on these issues, which should be public by default and could serve as a starting point for sector-specific discussions, codes of conduct, or traditional rule-making processes. These could benefit the wider ecosystem of concerned parties—including Congress, peer agencies, and the courts—in seeking to understand and remedy consumer and competitive harms over time.

Newly empowered regulators can also play a role in shepherding data disclosure frameworks and standards that support researchers, global regulators, and the public in pursuing independent research of online services markets. Increasing access to academics and other qualified researchers is one of the few ways to allow for greater understanding of online services. There has been recent momentum in the EU and the United States to better address this information disparity, including the EU's Access to Data Held by Digital Platforms for the Purposes of Social Scientific Research working group,[239] new proposals for research of very large platforms in the EU's Digital Services Act,[240] and the United States' proposed Social Media Disclosure and Transparency of Advertisements Act.[241] Similar efforts to allow research access should be incorporated as part of general online services oversight responsibilities. Further coordination with global regulators around data disclosure standards could be particularly productive in catalyzing global understanding of shared challenges. Across research and investigation areas, regulators could develop and abide by standards and best practices for appropriately navigating the substantial privacy and intellectual properties sensitivities at play.

Referral and collaboration powers

In exercising new and enhanced investigative, oversight, and data disclosure authorities within online services markets, regulators may encounter issues that are pertinent to other state or federal agencies. To maximize both new and

existing agency powers in service of the public interest, regulators should have referral powers to bring issues, conduct, or other pertinent information to the attention of other government agencies. Referrals should always be made wherever potentially unlawful conduct is found under other existing statutes.

In many cases, sector-specific regulators may currently be responsible for regulating activities occurring in part on online platforms—such as advertising employment opportunities—without the informational awareness or technical expertise to fully address them. For this reason, the entity charged with administering the general online services regulatory model should serve as both a center for expertise on online services and a partner to other agencies as they include aspects of online services in their sector-specific regulations. In so doing, the general online services regulations can provide common elements and principles for integration. These collaborations could deconflict online services regulatory approaches across the whole of government. As noted above, online services regulators would also have robust investigative and referral powers and could shine a light on problems for other agencies to address.

For example, existing sector-specific regulators, such as the National Highway Traffic Safety Administration (NHTSA), oversee self-driving cars and automated vehicle technologies.[242] As these efforts evolve, NHTSA could leverage online services principles, standards, or regulations in their efforts, or at minimum, ensure that they are not in conflict. Similarly, an online services regulator that discovers issues in the online services used by self-driving cars, such as insecure software or deceptive claims of system performance, would be able to refer them to NHTSA and, if needed, coordinate on addressing identified harms.

Through these referral and collaboration processes, regulators can assist a range of federal and state bodies in making existing regulations robust against emerging and future problems. There is ample precedent for such an approach. For example, the Federal Deposit Insurance Corporation is responsible for supervising all chartered banks, with a range of accompanying enforcement powers to do so. It examines these banks not only for safety and soundness, but also for compliance with more than 20 different federal consumer protection statutes—even statutes for which other agencies are the primary regulators. In areas where no other entity has responsibility to guard the public interest, dedicated rule-making responsibilities will enable online services regulators to ensure that challenges raised by online services do not fall through the cracks.

Rule-making powers

For online service providers that do not choose to be classified as online infrastructure, Congress should empower an expert administrative body with robust oversight and rule-making powers guided by the legislatively enumerated regulatory principles described below. (A discussion on selecting a body continues below in "Administering regulation.") However, as general principles on their own are insufficient to guard against industry capture and ensure clear administrability, each category should also include more specific per se violations that create clear guardrails. For example, the House Judiciary Antitrust Subcommittee's tech antitrust bills and new Senate companion bills[243] put forth a number of rules around nondiscrimination that would make this behavior unlawful for dominant online platforms; such a rule exemplifies the type of guardrail where Congress fully understands a problematic activity at the time of drafting a statute. Further work will expand on proposed clear-cut statutory rules and examples of rule-making additions for each of these spaces.

Critically, this regulatory model would have the ability to create rules for all players in online services markets. Much of the focus on curbing the tech sector's abuses have centered on the largest gatekeeper companies. However, abuses can happen from all players in the ecosystem, including users, vendors, advertisers, and smaller business. Where harms are widespread, having rules that apply to everyone is critical to ensuring the development of a stronger, safer, and more vibrant online services ecosystem.

Thus, some new statutes and accompanying rule-making activity may create clear rules and regulations for online services generally. But much of this activity would likely be targeted at specific markets, technologies, or submarkets. Within the broader ecosystem of online services, it is likely that different types of online services will require different sets of rules for their individual, sector-specific markets. Problems in the augmented reality market, for example, will likely require some different rules and remedies than markets for IoT devices or AI. As a starting place for oversight and rule-making, Congress should designate initial sector-specific markets where it suspects regulatory intervention is overdue based on the principles below. The entity or entities in charge of administering this regulation should be able to select future markets for this purpose. Specific selection criteria for initial focus markets will be the subject of further work.

Principles for online services rules

The Center for American Progress' proposed approach is a hybrid one: Congress would both define specific practices that would be explicitly outlawed and enumerate broader principles around which regulators could interpret and craft rules. For example, Congress might explicitly prohibit the sale of biometric data but also more generally prohibit insecure and data extractive practices; a regulator might then promulgate a rule prohibiting firms from scraping photos from online services without securing users' permission to build a facial recognition service for clients. The combination of clear guardrails and the flexibility of a principles-based approach offers flexibility to address future problems and mitigation of any industry capture of the regulator.

Similar principles-based approaches have been used to regulate financial services. Building on a robust separation regime, the federal government empowers financial regulators with flexible rule-making capabilities, in theory enabling them to address unanticipated, emergent threats. Agencies charged with regulating financial institutions or their products—such as the Federal Reserve and the Consumer Financial Protection Bureau—have been empowered with broad supervisory and regulatory authority to ensure safety and soundness and guard against unfair and deceptive practices, respectively. This is critical because of the complexity of the financial sector and the inability for Congress to enumerate all of the potential mechanisms that could lead to systemic risk or consumer harm. Likewise, the speed of technological development in some online services markets can compound the existing challenges of needing specificity and specialized expertise, making multiple, flexible tools and ongoing oversight and rule-making responsibilities essential.

An online services regulator would promulgate rules in varied digital markets where harms arise on the basis of broad, statutorily-defined prohibited practices and factors that must be considered. Congress would describe these general categories of prohibited behavior—in addition to specific practices defined in statute to be unlawful for online services—and regulators would continue their work by developing and applying rules to specific technologies, practices, or markets, appropriately considering the requisite factors named as process requirements as new issues arise. Some of these principles intentionally overlap existing statutory areas. As noted under referral powers, many of these areas have yet to be clearly applied to the online services space, and new regulators will be a force multiplier in filling regulatory gaps and updating existing statutes. The first set of principles would take the form of unlawful prohibitions:

- **Anti-competitive practices:** Congress should explicitly make anti-competitive practices unlawful for online services generally and equip specialist regulators to promulgate specific rules for all online services, submarkets of online services, or various technologies. In response to the unique combination of factors that make digital markets prone to tipping and capture, this prohibition will help regulators more effectively promote competition and prohibit anti-competitive practices that are specific to digital markets. Competitive harms beyond consumer pricing should be considered, including competitive harms to both consumer markets and labor markets. In developing specific rules, regulators will need to balance rules around competition with rules around other principles, such as extractive data practices and privacy. Special concern should be given to small businesses, creators, and nonprofit services, whose prospects are powerfully affected by dominant players on which they may be dependent as business users or vendors.

- **Violations of civil rights:** In response to the history of tech companies showing negligence or defiance toward protecting civil rights, Congress must clarify an affirmative obligation for online services to protect all existing civil rights protections and explicitly prohibit any activity of these services that would have the effect of discriminating against protected classes, including through disparate impact. The online services regulator, in consultation with existing enforcement agencies, must be able to use its close proximity to and visibility into regulated entities to improve the enforcement of existing laws, including by promulgating rules prohibiting practices by online services that are likely to violate civil rights and identifying and preventing growing threats before they become widespread rights violations.

  Of course, civil rights violations are already illegal for online services. But considering the current enforcement gaps and the numerous impending threats to civil rights, additional mechanisms for clarifying and explicitly naming online services practices that pose civil rights risks are necessary. Clear rules, especially where case law may not yet be fully developed, can eliminate the argument that there are any open questions where rights are at risk. Clarity and explicit naming of violative practices in rule-making may enable more robust enforcement, making it easier to bring actions where harms have occurred and catalyze swifter progress on the application and understanding of civil rights online. Congress should be clear that existing civil rights laws and regulations are a floor for any regulations added by online services regulators, in consultation with existing civil rights agencies, to clarify how they should be applied to online service provision.

- **Insecure and data-extractive practices:** Regulators should be empowered to curb dangerous, insecure, or data-extractive practices. A new federal privacy law may cover some or all of this territory, but the mass surveillance, collection, processing, and use of extractive practices unnecessarily threatens rights and creates dangerous industry standards in evolving ways. Regulators should be empowered with the ability to create new rules that protect privacy rights in emergent settings as necessary; modern privacy protection will require dynamic, systemic solutions beyond individual-level data protection.

- **Unfair, deceptive, abusive acts or practices for consumer and business users:** In response to the history of harmful consumer practices becoming industry standards within digital markets, Congress should make illegal—and regulators should proactively protect consumers from—unfair, deceptive, or abusive acts or practices. Online services regulators should have a special focus on setting cybersecurity baselines, which other consumer protection bodies are less well-positioned to do.

Furthermore, the list of principles could include some combination of the following factors that regulators are required to consider in the development of specific rules. In many cases, rule-making can simultaneously advance all of these principles, but in others, explicit balancing across principles and weighing of any tensions or trade-offs will be required. In addition to the lawful prohibitions outlined above, this proposal aims to outline the start of an affirmative public interest mandate for online services regulation. Including such public interest considerations furthers the robust regulatory tradition of explicit, affirmative public interest obligations for U.S. regulatory bodies:

- **Equitable growth:** In response to the way that the benefits of and wealth from digital innovation have disproportionately accrued to privileged groups,[244] regulators should incorporate consideration of whether new rules made in response to the above principles will promote equitable or inequitable growth. Where possible, regulators should consider a rule's potential impact in its development, favoring rules that promote equitable economic growth and wealth-building that benefit a broader population of Americans rather than rules that would continue to entrench economic inequality.

- **Innovation:** In response to the benefits of digital innovation and the threats to progress posed by anti-competitive practices, regulators should incorporate broad, long-term consideration of whether new rules promote or hinder research and innovation.

- **Representation of all participants:** Digital markets often contain different types of participants, including consumer users, workers, business users, vendors such as advertisers and sellers, and the platform entity running the market or digital property. In making rules that apply to these markets, the interests of all of the participants should be considered, not just those of the most well-resourced or well-organized constituents. Digital advertisers, for instance, have far more resources to advocate for their desired outcomes than platform workers or small businesses. In balancing competing interests, regulators should take special consideration of harms to individuals or classes of individuals over harms to corporate entities.

- **Information diversity and pluralism:** In recognition of the unique societal and democratic challenges posed by concentration of informational and communications infrastructures, independent regulators should consider whether rule-making unnecessarily contributes to the concentration or degradation of information and communications infrastructure and instead seek to promote diversity, quality, and pluralism of online services.

Dedicated, expert regulators would promulgate rules that consider these factors when seeking to operationalize the classes of prohibitions enumerated by Congress, turning general principles into rules that address the specifics of different technologies and online services markets. Regulators will invest in expertise to understand the complexity and variety of the online services space, bringing together the technical, social, economic, and legal knowledge required to effectively govern it. In doing so, they will be informed and engaged enough to strike an appropriate regulatory balance among risk, growth, and competing objectives in burgeoning online services industries. They will identify common problems across disparate industries and consult with other regulatory bodies in their own rule-making. Together, this should give regulators sufficient rule-making authority over online services and the expertise necessary to govern them effectively. These authorities would complement, not supplement, existing FTC, DOJ, and other sector-specific jurisdictions over related issues.

Principles-based rule-making in practice

As noted, while some rules may apply to all general online services, many will likely be targeted by a specific technology or submarket. Looking ahead, it is easy to imagine instances where principled rule-making and expert oversight could be used as appropriate complements to address the economic, privacy, consumer protection, and civil rights harms outlined earlier in this report. To help bring to life new rule-making powers, consider the below examples:

Rules preventing anti-competitive practices: Early intervention could help prevent anti-competitive default agreements in emerging digital hardware properties such as VR or smart home tech. This would prevent gatekeepers like Google or Facebook from paying for default rights at every new opportunity—for smart TVs, smart speakers, smart refrigerators, VR environments, wearables, and other products—and avoid prolonged, ex-post litigation from undoing those agreements 10 years too late.

Rules preventing data-extractive practices: Regulators could provide helpful nuance and accompanying rules in the debate over data scraping. They might add to the conversation by defining acceptable use—for example, privacy-preserving research—or by explicitly prohibiting inappropriate activities, such as the case of Clearview AI scraping and selling biometric data products built on publicly available information without people's consent.

Rules preventing insecure practices: Baseline cybersecurity rules and standards developed in conjunction with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the U.S. Department of Commerce's NIST could help end the race to the bottom occurring in emerging technologies such as IoT, curbing the disastrous boom of consumer electronics that are insecure by default.

Rules around unfair, deceptive, or abusive acts or practices for consumer users: Consumer protection concerns around the ongoing use of dark patterns could be sustainably addressed, clearly delineating between appropriate digital sales techniques and tactics that cross the line into deception—that is, unfair, deceptive, or abusive acts or practices.

Rules around unfair, deceptive, abusive acts or practices for business users: Regulators could restrict platform use of business transaction data in an online marketplace to competitively benefit first-party services or products over third parties, unless third-party services or products also receive sufficient access to that data.

Rules around violations of civil rights: Regulators could put affirmative burdens on online services providers to demonstrate that their machine-learning algorithms do not produce disparate impacts for protected classes prior to deployment.

Rules encouraging innovation: Sector-specific rules or collaborative codes of conduct could help support the development or adoption of shared standards in emerging media formats or digital markets, such as digital identity or algorithmic auditing standards, to promote competition and avoid lock-in for consumers.

Additional responsibilities for gatekeeper services

A few companies achieved early success in new sectors of the digital economy and now dominate much of the consumer internet. Recent scholarship on digital gatekeepers has disentangled the natural features of digital markets that support capture and tipping from the anti-competitive actions companies may take to exploit those features. Digital markets are characterized by strong network effects, extreme economies of scale and scope, high barriers to entry, and acute information asymmetries between dominant platforms, dependent players, and Americans who rely on these services every day.[245] While the individual characteristics of digital markets are nothing new, the combination of these features and the degree to which they play out online poses acute challenges to market function and heavily favors dominant digital incumbents.[246] In the vacuum of regulation and antitrust enforcement in recent decades, some dominant companies have abused natural market conditions to kill competitors, entrench dominance, stave off regulation, chill innovation, and continually leverage their dominance into adjacent sectors of the economy. Consumers—and the hundreds of thousands of small and medium businesses and digital creators that are reliant on these companies to reach them—have lost out.

Looking solely at economic outcomes does not fully capture the risks posed by digital gatekeepers. Very large digital gatekeepers are systemically important, as their actions have major implications for the U.S. economy, society, and security. Similar to systemically important financial institutions, they pose widespread risks given their status as functionally essential and ubiquitous informational infrastructure. Abusive behavior toward consumers, potential competitors, or corporate negligence on a range of critical public interest issues—such as cybersecurity, data privacy, discrimination, political advertising, content moderation, and site reliability—can generate cascading social harms and significant economic costs. Americans want, and regulators should provide, oversight over digital gatekeepers that have the potential to cause massive harm—especially in those areas where harms are unseen or diffuse.[247] Given their scale, such platforms should not be allowed to operate in ways that are fundamentally contrary to the public interest. While a robust and complex conversation is needed on what should constitute appropriate and rights-respecting forms of oversight and regulation in response to risk, the need for oversight is clear. The EU's Digital Services Act,[248] a recent legislative proposal that explicitly incorporates language around risk and due diligence for very large online platforms, grapples with similar issues.

The Center for American Progress has previously written in favor of more aggressive antitrust action[249] and robust competition policies,[250] including statements of support for the package of antitrust and competition bills reported out of the House Judiciary Committee in the 117th Congress that tackle digital gatekeepers. These bills, led by Chairman David Cicilline (D-RI) and informed by the subcommittee's report on digital platforms,[251] are a direct response to the problems outlined above. The Ending Platform Monopolies Act, which addresses underlying conflicts of interest between platforms and commerce, provides a unique opportunity to change foundational incentives for dominant platforms, rather than needing to monitor behavior in-depth on an ongoing basis. The American Choice and Innovation Online Act and new companion legislation led by Sen. Amy Klobuchar (D-MN) would introduce nondiscrimination provisions and restrictions on self-preferencing, offering an opportunity to curb many of the competitive abuses to small businesses outlined above.[252] These bills present the 117th Congress with a meaningful opportunity to address some of the most troubling abuses of gatekeeper power.

Considering the importance of gatekeeping firms to the U.S. economy and the propensity for digital markets to tend toward tipping, the U.S. should consider *additional* laws and regulatory scrutiny of such firms going forward. Indeed, because antitrust enforcement in digital markets has been so anemic, it is possible that even after separation, a number of firms would still qualify as digital gatekeepers as conceptualized below. Additional regulatory scrutiny can ensure a range of harms and risks are sustainably addressed, including and beyond those firms that have gatekeeping power but could be dealt with through structural approaches. To determine which firms deserve additional regulatory scrutiny, this report builds on existing scholarship—including the House and Senate tech antitrust package and the EU's Digital Markets Act—to propose a test that could be used to identify future gatekeepers. Following the test, this report suggests further regulation and risk mitigation tools that may be brought to bear on qualifying gatekeeper services.

Gatekeeper test

Recent scholarship and government investigations from around the globe have coalesced around a set of factors that characterize digital gatekeepers, but articulating a precise definition is the subject of ongoing legal and policy work. As described by FTC Chair Lina Khan, "Gatekeeper power can arise any time there is a network monopoly, a feature of industries with high fixed costs and network effects, or the phenomenon whereby a product or service becomes more valuable the more that users use it."[253] In the context of online services or tech platforms,

she notes, "While more extensive studies of platform power would benefit from being platform-specific, identifying the common bases of their dominance helps place them within existing legal frameworks. The first is gatekeeper power. This power stems from the fact that these companies serve effectively as infrastructure for digital markets—they are distribution channels, the arteries of commerce. They have captured control over technologies that other firms rely on to do business in the online economy."[254] Acknowledging the divergent forms of gatekeeping that arise from a similar set of conditions in digital markets, a test that covers multiple conditions is preferable to a single cookie-cutter definition.

In order to formulate such a test, this report surveyed major research reports and legislation targeting digital gatekeepers in recent years: the University of Chicago Stigler Center Committee on Digital Platforms report,[255] U.S. House Antitrust Subcommittee report,[256] U.K. Digital Competition Expert Panel report,[257] U.K. Competition and Markets Authority report,[258] Australian Competition and Consumer Commission digital platforms inquiry report,[259] French Competition Authority digital platforms report,[260] Germany's 19a antitrust policies,[261] European Commission's digital era competition report,[262] EU's Digital Markets Act,[263] Japan's Ministry of Economy, Trade, and Industry digital platforms regulation,[264] Harvard Shorenstein Center proposal,[265] Brookings Institution big tech regulation report,[266] Public Knowledge Digital Platform Act,[267] and Washington Equitable Growth antitrust and competition report.[268] This report catalogued the definitional proposals across reports and identified the named characteristics for harmful digital gatekeeping in each.

Building on this foundation, each characteristic was considered in light of their regulatory feasibility in the United States. After exploring various approaches to combining these factors—comparing them with the existing landscape of digital gatekeepers and imagining the likely gatekeepers of tomorrow—the authors developed the following digital gatekeeper test to identify gatekeepers that pose unacceptable risk to the public interest. The EU's Digital Markets Act and the U.S. House tech antitrust legislative suite,[269] released midway through this report's own development, provided useful comparisons, and some elements are echoed in this proposal.[270]

In order to be subject to gatekeeper regulations, firms would first have to meet the definition of online services in a primary business unit.[271] Many qualifying gatekeepers will operate multisided markets, but other large, dominant online businesses or ubiquitous, systemically important services may also qualify.

Eligible companies will qualify for gatekeeper status if three of the four conditions below are met. While each is an important part of the puzzle, every condition also has a predictable counterexample that means it is not necessary to establish gatekeeper power in *all* cases. Due to the extreme economies of scale and scope in digital markets and the prevalence of cross-subsidized business lines, either the provider overall *or* only one of a provider's business lines needs to meet the requirements. These thresholds are provided for illustrative purposes; whatever criteria are chosen, regulators will need the ability to update specific quantitative thresholds based on market developments and economic changes over time. These ideas are meant to be further data points in the continuing conversation about how best to turn well-established economic observations and criticisms on digital gatekeepers into a functional, empirical regulatory test that effectively targets products with harmful gatekeeping power.

TABLE 1

Online services providers must meet at least three of the following four thresholds in a business line to qualify as gatekeepers

The digital gatekeeping test

Condition	Threshold
Significant impact on national economy	At least $9 billion in U.S. annual revenue in the last three years or at least $90 billion U.S. fair market value or average market capitalization in the last financial year
Significant market power	30 percent or greater market share or "q ratio" (or Tobin's Q)* above two
Key intermediary or critical trading partner	10,000 active U.S. business users in the previous year and 30 million monthly active users in the United States or a critical buyer or seller holding 50 percent of a critical market upon which upstream or downstream markets are dependent
Durable market influence	Met any of the above conditions in each of the past three years

**Tobin's Q is a ratio expressing a firm's market value divided by the replacement cost of the firm's capital assets.*

Condition #1 accounts for an online services provider's sheer economic importance to the United States. The first threshold of $9 billion in U.S. annual revenue in the past three years and the second threshold of $90 billion in fair market value or average U.S. market capitalization in the past financial year mirror the EU's Digital Markets Act proposals around economic importance, scaled to U.S. market size; the Digital Markets Act threshold of €65 billion used the average market cap of the EURO STOXX 50, adjusted for future growth expectations. The House's American Choice and Innovation Online Act, which set the threshold at $600 billion, does not present a direct comparison here given its global scope.

Such a figure might be indexed to growth or calibrated to consistently capture above-average market caps for a group of the largest U.S. companies over time. In considering potential counterexamples, a product's technological importance might grow more quickly than its economic performance, and thus monetary impact on the national economy may not always accurately reflect a product's true importance in the short run.

Condition #2 accounts for products whose market power affords them gatekeeping power. Firms can qualify either with a market share above 30 percent or a Q ratio, also known as Tobin's Q, that is consistently higher than 2. At 30 percent market share, this threshold aims to capture not only firms that hold monopoly or duopoly power, but also firms that dominate markets as part of an oligopoly. However, market share has increasingly come under scrutiny as a standalone indicator of market power. And online services firms have tended to complicate the process of market definition through multisidedness, zero-price services, and data economies. The variation in business models among digital gatekeepers further indicates that multiple indicia of market power may be needed. Thus, a firm can also qualify by exhibiting a Q ratio greater than 2.

Tobin's Q is the firm's market value divided by the replacement cost of the firm's capital assets.[272] As explained by Marc Jarsulic and others, persistently high Q ratios are one indicator that a firm is extracting monopoly rents.[273] When financial market valuations exceed capital costs, there is an incentive to buy assets and employ them in that line of business. In a competitive market, entry should continue until increased supply lowers returns and the Q ratio declines to one. The Peters-Taylor methodology of calculating Q, which includes intangible capital in the denominator of Q, is a sensible approach to valuing online services companies, for which intangible assets are significant.[274] Setting the threshold at 2 essentially says that if a company is persistently valued by financial markets at a level that is *more than double* the worth of its assets, firms are earning economic rents that indicate significant market power.[275] Given the free and multisided nature of many digital services, Q ratios are a useful metric for understanding the market power of digital firms.

In addition to these two indicators, regulators should be empowered to establish more stringent standards through rule-making processes as markets evolve. The Digital Markets Act and the American Choice and Innovation Online Act both acknowledge the importance of market power generally. Most gatekeepers will likely have significant market power, but there are cases where gatekeeping power may arise prior to a product's market capture or absent a clearly definable market; therefore, condition #2 is expected in most, but not necessarily all cases.

Condition #3 speaks directly to a product's intermediation power. The threshold seeks to target services that play economically important intermediation roles based on high numbers of monthly active users and business users or based on holding significant market power in a strategically critical market. This proposal's threshold for the number of U.S. business users—10,000—reflects the EU's business threshold in the Digital Markets Act, which was itself calibrated to represent a small share of the entire population of "heavy" business users on EU platforms. The number of monthly active U.S. users, 30 million, represents approximately 10 percent of the U.S. population, which is also slightly below the threshold in the American Choice and Innovation Online Act of 50 million monthly active U.S. users. The threshold for critical buyer or seller market share, 50 percent, represents a point above which courts have tended to find monopoly power.[276] Further research is needed to identify the particular characteristics of economically powerful and systemically important digital intermediation services, but in the absence of clearer tipping points, a descriptive but conservative approach could be a good starting point. A small but ubiquitous and highly interconnected firm may exercise robust intermediation power, and whatever metrics are chosen should reflect this possibility. Most digital gatekeepers are expected to meet condition #3, but it is possible that an online service could acquire gatekeeper influence through sheer economic size, market dominance, and market durability, rather than having a literal intermediation position.

Condition #4 introduces the traditional "durability" metric, scaled to three years to account for the swift pace of digital markets, as a final indicator of gatekeeping power. The Digital Markets Act proposes a similar approach to durability. Incredibly popular products could foreseeably arise and amass gatekeeper power in less than three years. Thus, condition #4 will likely be met in many but not all cases.

TABLE 2

Sample illustration of the gatekeeping test with company-by-company estimates

Gatekeeper conditions: ✘ Unlikely to qualify ✔ Likely to qualify ? Insufficient data

	Significant economic impact	Significant market power	Key intermediary or critical trading partner	Durable market influence	Projected result
Apple	✔	✔	✔	✔	✔
Amazon	✔	✔	✔	✔	✔
Google	✔	✔	✔	✔	✔
Facebook	✔	✔	✔	✔	✔
Microsoft	✔	?	✔	✔	✔
Netflix	✔	?	✘	✘	✘
Walmart Marketplace	✔	?	✔	✔	✔
Target+	✔	?	✘	✔	✘
Spotify	✘	?	✔	✘	✘
Etsy	✘	?	?	✘	✘
Yelp	✘	?	?	✘	✘

Note: Estimates of likely qualification are provided strictly for illustrative purposes based on limited available data. Companies must meet three criteria to qualify as gatekeepers.

Sources: Authors' analysis based on limited available data at the time of publication. A full list of sources is available at https://cf.americanprogress.org/wp-content/uploads/2021/11/OnlineServices-sources.pdf.

Gatekeeper governance

In crafting regulations, Congress and relevant regulators—whether through the pending tech antitrust bills or as part of a future comprehensive regulatory statute—should reign in anti-competitive practices and consumer harms that are uniquely enabled by gatekeeper status, above and beyond any rules proposed through general online services regulations. Specifically, goals for gatekeeper regulation should include:

1. Preventing gatekeeper companies from further increasing market dominance
2. Preventing gatekeeper companies from abusing market dominance to harm competitors, potential competitors, consumers, and workers
3. Promoting competition by increasing market access and lowering barriers to entry for potential competitors, especially small and medium competitors, without unnecessarily impairing gatekeepers' ability to act freely
4. Mitigating significant, systemic risks posed by gatekeeper companies to the national interest, including the national economy, cybersecurity and informational infrastructure, democratic infrastructure, public health infrastructure, and fundamental rights

To achieve these gatekeeper goals, both structural and functional separation should be utilized where appropriate. In her 2019 article, "The Separation of Platforms and Commerce," Khan described operational or functional separation and structural separation as such:

> *An operational or functional separation requires the firm to create separate divisions within the firm, requiring that a platform wishing to engage in commerce may do so only through a separate and independent affiliate, which the platform may not favor in any manner. A full structural separation, by contrast, requires that the platform activity and commercial activity be undertaken through separate corporations with distinct ownership and management.*[277]

Khan makes a persuasive case for reviving structural separation approaches for digital markets, particularly in light of the challenges in functional separation.[278] Indeed, when determined by the courts or clearly laid out in statue, structural separation is a preferred strategy for grappling with fundamental anti-competitive conflicts of interests within digital platforms, although it has been infrequently used in recent decades.

Structural separation approaches for gatekeepers should continue to be initiated through antitrust litigation or in clearly defined statutes, such as in the proposed Ending Platform Monopolies Act.[279] A regulatory entity with the ability to determine structural separation without clear statutory guidelines, however, raises the risk of potential abuse and inevitable legal challenges.[280] Rather, additional tools for an online services regulator may include reviewing or overseeing, but not initiating, separation regimes.

Agency regulators tasked with gatekeeper oversight might also be given the ability to initiate functional separation. In some circumstances, functional separation could be the maximal appropriate tool for a dedicated regulator to level on a gatekeeper—preserving structural separation as an option through antitrust enforcement or when explicitly directed by statute in cases of unavoidable conflicts of interest. Functional separation, with its tradeoffs, may be less effective and more difficult to administer than structural separation, but should be preserved as a tool in the regulator's toolbox when structural separation may not be possible.

Additional gatekeeper tools

Beyond structural and functional separation approaches, further strategies employed in gatekeeper oversight should include restrictions on self-preferencing, bundling, price discrimination, interoperability and data-sharing rules, and enhanced disclosure obligations tailored to particular forms of gatekeeping power, among others:

- **Restrictions on self-preferencing:** Identify and prohibit competitively relevant self-preferencing practices. These might relate to search rankings, web display locations, data withholding, and tiered web, software, or operating systems that offer superior performance to interoperating first-party services. This could include prohibitions on the foreclosure or restriction of consumer communication channels, such as those that have been used by some platforms to prevent developers from growing business relationships with consumers off-platform.

- **Restrictions on bundling of goods or services:** Place restrictions on what goods or services digital gatekeepers can bundle together in cases where bundling creates anti-competitive market effects.

- **Restrictions on price discrimination:** Place restrictions on pricing discrimination practices where gatekeepers are maintaining or abusing market dominance over business or consumer users. Given the unprecedented level of consumer data collection, processing, and targeting capabilities, these rules are especially important for maintaining healthy, competitive digital markets.

- **Bans on unfair trading practices:** Institute tailored restrictions on gatekeepers that are maintaining or abusing market dominance through unfair trading practices, especially in their dealings with platform business users.

- **Terms of service for business users:** Prohibit unfair or harmful practices and encourage pro-competitive terms for business users, such as ending self-preferential data hoarding, instituting dispute resolution systems, or providing greater transparency around algorithmic sorting practices.

- **Terms of service for consumer users:** Prohibit unfair or harmful practices toward consumer users, such as surveillance and privacy violations, dark patterns, and algorithmic discrimination.

- **Interoperability requirements or incentives:** In cases where it would ameliorate clear areas of competitive or consumer harms, require or incentivize increased interoperability with other services and prohibit practices that would prevent competitors from effectively interoperating. Regulators with enhanced capacity, investigative powers, and rule-making ability would be well positioned to effectively balance the concerns among privacy, security, and competition. Another bill in the House tech antitrust package, the Augmenting Compatibility and Competition by Enabling Service Switching Act, includes such interoperability and data portability provisions.[281]

- **Data portability requirements:** Require data formatting and export features that would allow consumers or business users to take usable copies of platform-specific digital properties to a competing service. Portable digital properties might include algorithmic preferences or a user data corpus, such as posts, multimedia, or information about a user's contribution to the service over time. Again, balancing values and navigating long-standing challenges around privacy, consent, and IP issues within data portability requirements would be an ideal task for online services regulators.

- **Enhanced transparency and disclosure obligations:** Impose additional disclosure or data-sharing requirements, for public use and regulator use, on business or platform practices relevant to regulator goals. These could include disclosure on cross-subsidization of business lines, greater data sharing on harmful treatment of priority consumer groups, or transparency on algorithmic design.

- **Enhanced oversight obligations:** Similar to the Securities and Exchange Commission or the U.S. Department of Agriculture, regulators could embed "on-the-line" inspectors—whether on the assembly line or the command line—to learn more about business practices of interest or enforce gatekeeper obligations. With confidentiality rules to protect intellectual property, enhanced oversight could greatly aid understanding of public interest matters and enforcement of new regulations in specialist areas at the software or algorithmic management levels.

- **Referral for antitrust scrutiny:** While regulators should be empowered with a number of tools to end anti-competitive practices, cases that require additional scrutiny or result in remedies outside of the online services regulation mandate may require referrals to the FTC, DOJ, or state attorneys general.

- **Regulatory referral:** All of the proposals here are meant to be complementary to existing regulations on labor, civil rights, commerce, telecommunications, financial products, and other sector-specific rules. In cases where issues are better handled by another sector-specific agency, referrals should be made to the appropriate body for further action, including sharing any data, insights, or personnel that might aid a peer agency in its work or, in some cases, directly bringing an action in the federal courts. A dedicated online services regulator may be well placed to implement a general reporting system for online services issues and aid in routing such complaints to appropriate federal bodies.

While some of the harms from dominant digital gatekeepers can be alleviated by industrywide rules and baselines imposed on general online service providers, others will require dedicated scrutiny. Due to the regulatory debt built up around gatekeepers and their economic importance, one-size-fits-all rules cannot always capture the issues posed by particular gatekeeping powers. In addition to clear rules wherever possible, a regulator with the mandate to examine the best way to preserve and balance the principles set forth by Congress, with the flexibility to evaluate specific types of gatekeeper power, would be a useful complement to reinvigorated antitrust action in the digital platform space.

Addressing content regulation challenges

The instantaneous speed, amplification, discovery, and relational nature of speech online are at the heart of the productive and transformative capabilities of the internet. But the rise of gatekeeper platforms means that many of the world's online interactions are intermediated by a handful of companies whose decisions profoundly affect how people communicate and whose business incentives cut against the public interest. In particular, negligent business models that amplify, promote, and target content to certain users are accelerating societal divisions, compounding existing inequities, and sustaining extractive surveillance business models. These systems have been easily exploited by malicious actors for purposes of harassment, voter suppression, and disinformation, adding even greater urgency to long-standing problems.

The regulatory proposals in this report and the relevant tools outlined below focus on how online services treat consumers, creators, business users, workers, and competitors. They do not constitute a program of direct speech regulation. Instead, this framework creates the capacity for regulators to identify clear risks, including systemic risks, and address them through the lenses of consumer protection, civil rights, and competition. These are long-standing regulatory and oversight traditions that can address specific issues as they are—for example, abusive business practices, deprivation of rights, or anti-competitive practices. They offer sensible, legal interventions related to many, though certainly not all, issues included in the locus of discussion around so-called harmful but legal online content. These traditions may offer a more tractable lens than that of speech regulation, which will face steep challenges in the courts.

Many of the tools below target the troubling information asymmetry between private online services providers and everyone else. These providers are profoundly influential in shaping public discourse. Their refusal to provide the public, regulators, or researchers with even basic data about their business practices and programs is a foundational rejection of their public interest responsibilities.

The apparent misrepresentations that some providers have willingly made to the public and even Congress are likewise deeply troubling.[282] A regulatory entity with the tools to bring transparency, research, and understanding to this space can be catalytic in illuminating potential remedies.

In unpacking how those tools apply to harmful content online, it is helpful to disaggregate the term into specific issues. Myriad problems tend to get lumped together in this discussion, particularly as they relate to reform or repeal of Section 230 intermediary liability protections. These include but are not limited to harassment, hate speech, scams, discrimination, fraud in advertising, doxxing, algorithmic transparency, misinformation, disinformation, voter suppression, radicalization, election interference, or nonconsensual pornography. Each of these is a serious issue meriting dedicated consideration. Americans' online interactions are real, innumerable, and complex: Legal and regulatory systems do not try to address embodied actions of harassment, voter intimidation, discrimination, and public health interference with a single policy response; neither should they do so with their digital instantiations. To better craft policy responses to these issues, regulators must widen their aperture beyond a flattened idea of "content" to look upstream at business models and design choices, downstream at the relational harms or other direct impacts on individuals, and broadly at the historical context and information environment that online service platforms create.[283] Section 230 is one part of this ecosystem—and perhaps the most discussed given that Congress does have leeway under the First Amendment to change intermediary liability rules—but is not the whole ballgame.

New regulatory tools might be able to address various aspects of specific problems, such as deceptive design, negligent business practices, infringement of rights, abuses of market power, or the need for greater redress or understanding. An online infrastructure regulator might impose public interest transparency reporting or staffing obligations to enable rights-respecting treatment of illegal content among infrastructural providers. A general online services regulator might bring to bear enhanced investigatory and rule-making powers wherever technologies or business practices are anti-competitive, unfair, deceptive, abusive, insecure, data extractive, or likely to violate civil rights. The requirement to consider effects on information diversity within online services rule-making will ensure that new rules promote pluralism over continued concentration. Additional gatekeeper rules for the largest and most important players will provide further oversight and systemic mitigation of risks to national cybersecurity and democratic infrastructures, among other critical systems.

For purposes of illustration, concrete uses of these tools might include:

- **Impact assessments:** General online services may conduct expert impact assessments. Allowing for point-in-time assessments and tracking of persistent issues over time could inform independent study and public understanding of issues. For example, regulators might investigate the effect of particular social media platform designs, business practices, or interventions on the dissemination of quality public health information and the large-scale spread of public health misinformation during the COVID-19 pandemic.

- **Rule-making against consumer protection harms:** General online services regulators could introduce new consumer protection standards for a variety of abusive and harmful practices. These could include, for example, standards for consumer protection and redress for social media users targeted by harassment or hate.

- **Rule-making against civil rights harms:** General online services regulators could introduce new rules and standards to guard against violations of civil rights online. For example, regulators could promulgate rules establishing efficacy and implementation standards for the protection of civil rights in algorithmic development and deployment or in digital ad delivery and targeting of businesses.

- **Systemic risk regulation for gatekeepers:** Providers that qualify as gatekeepers may be subject to additional restrictions to mitigate systemic risks to the national interest and national infrastructure systems. Interventions may be put in place to prevent scaled failures of systems that would undermine critical cybersecurity infrastructure or democratic infrastructure. For example, finding systemic vulnerabilities within digital advertising systems that could enable foreign election interference could trigger required enhancements for vulnerable gatekeeper providers. Similarly, systems vulnerabilities that could enable scaled voter suppression programs may face new business restrictions, required process upgrades, or mandatory reporting programs.

- **Cooperative codes:** Regulators could help spark and coordinate the development of cooperative codes. Around these issues, stakeholders might work together on a voluntary basis to create and steward cooperative standards around transparency commitments, content moderation best practices, risk mitigation around foreign interference, or approaches to cross-platform abuse or hate speech. Such standards would need to build on lessons learned in related efforts regarding transparency, due process, and government coercion.[284]

- **Audit checks:** At present, there is little assurance that platforms are faithfully representing their activities in public transparency reports or in stated standards and terms for users. Audit checks could greatly add to public confidence in and understanding of online services, particularly as they relate to the sensitive issues around harmful content, over-moderation, and user redress.

- **Transparency coordination:** There may be a role to play for general online services regulators in helping coordinate and standardize research access and public disclosures for global regulators, academics, and the public. Regulators may be well-positioned to figure out what transparency should look like for various online businesses and grapple with the important tensions among transparency, privacy, and intellectual property.[285]

- **Expertise, investigations, and referrals:** As part of their oversight obligations, regulators may conduct investigations into critical issues and, where necessary, serve as an expert partner on efforts by other government entities in understanding and protecting the public interest in their areas of work. These inquiries may touch on various issues related to harmful online content, such as understanding online voter suppression or foreign influence operations, in partnership with relevant agencies such as the DOJ or FEC.

Going forward, First Amendment protections, the risk of government abuse in speech regulation, American values, and the history of the government's failure to protect the expression of oppressed Americans should inform a difficult calculus for online speech regulation. While the goal of protecting freedom of expression is clear, the best means to achieve it is an open debate. How should society treat speech that seeks to undermine the very idea of public discourse itself? What is an appropriate, rights-respecting role for government within that treatment? A favorite U.S. adage suggests that the best antidote for harmful speech is more speech. But automated, instantaneous global amplification and surveillance-driven targeting that are used to uplift, silence, or drown out other voices begs the question of whether protecting freedom of expression requires approaches that accommodate, rather than ignore, the ways technology has changed how people communicate.

But automated, instantaneous global amplification and surveillance-driven targeting that are used to uplift, silence, or drown out other voices begs the question of whether protecting freedom of expression requires approaches that accommodate, rather than ignore, the ways technology has changed how people communicate.

An entity with the tools to bring transparency, research, and understanding to this space is one that can illuminate potential remedies going forward. Especially as the conversation around reform or repeal of Section 230's intermediary liability protections continues, gaining greater understanding of the impacts of reform can aid in aligning outcomes with policy goals. In particular, increased transparency on platform moderation practices will be needed to assess the effects of any carefully calibrated updates. Additionally, if there are very narrow, specific issues that are so severe that they merit changes to speech regulation by Congress, such proposals would only be upheld by the courts with overwhelming evidence of harm. Thus, the full range of possible actions in this realm will require clearer evidence on harms and tradeoffs. Greater understanding can aid lawmakers and the public in assessing proposals on their merits.

Even as the national discussion about the government's role in guarding freedom of expression online continues, more clear-cut regulatory approaches grounded in civil rights, consumer protection, competition, and dramatically stronger transparency standards are appropriate responses in the immediate term. The proposals in this report outline a variety of sensible new tools for regulators to mitigate harm from online content problems. This rights-respecting approach is not totalizing, but it is a powerful, legal, and tractable place to start.

Administering regulation

Regulatory effectiveness faces a host of challenges, including regulatory capture, enforcement failures, difficulty for users, and a range of capacity and cultural constraints.[286] These factors present a strong argument for tools that are self-administering where possible, including structural separation and clear statutory lines for highly problematic practices. But as discussed above, there are limits to the ability of statutes to fully address the range, variety, and dynamism of some online services markets. Principles-based rule-making powers can offer a powerful complement to clear statutes in addressing complex, emerging issues and balancing conflicting priorities. New and existing statutes and rule-making powers will all need to be brought to bear in combination, despite the particular shortcomings of each. Shedding new light on longstanding administrability challenges is outside the scope of this paper. But going forward, these challenges should not be underestimated, nor should they serve as a barrier to action.

Expansion of existing agencies and consideration of new agencies should both be on the table. In either case, these proposals require significant expansion of the U.S. government's capacity and expertise. Given the complexity of some online services—many of which deal in technical fields relating to software engineering, machine learning, or algorithmic design—and their direct impact on Americans' access to opportunity, specialist regulators with appropriate sociotechnical expertise are required. The federal government must design a creative system that recruits needed expertise while sufficiently insulating agencies from industry capture. Such capacity will aid in making technologies more legible to the public, taking the air out of any unrealistic industry exaggerations of technical complexity and challenging unfounded objections to sensible regulation. Developing effective regulation will require wholesale rejection of the discriminatory industry dynamics—particularly around racial and gender-based discrimination—that are encoded and amplified throughout technologies, services, and products today.

Any additional responsibilities should be complementary and additive to existing DOJ, FTC, and FCC authorities, as well as sector-specific laws in other areas.

Creating a center of excellence within the executive branch for online services could be a catalyst to ensure that the U.S. government can holistically, effectively, and consistently regulate new technologies. Specialist regulatory entities could also provide needed expertise and common principles for use in other areas, such as housing, labor, or transportation.

While some responsibilities described in this report mark clear shifts from current work at existing regulatory agencies, others are more natural outgrowths. Going forward, administrative options could include:

- Expanding the powers of the FTC
- Expanding the powers of the FCC
- Expanding an executive branch agency, such as the National Telecommunications and Information Administration (NTIA), which is part of the U.S. Department of Commerce
- Vesting these powers in a new, independent regulator for online services
- Vesting these powers in whatever body is charged with administering any future federal privacy law
- A combination of the above approaches

For illustrative purposes, a brief tour of options is below.

Expand the FTC: An expanded FTC is in some ways a natural fit for these regulatory responsibilities. The FTC carries the dual mandate of competition and consumer protection. It looks holistically at these factors across large and small players and offers experience with issues around consumer data and privacy. And, as noted above, numerous proposals are already on the table to expand the FTC's focus on data protection and digital markets, whether through its own rule-making or expanded powers in federal privacy or competition legislation.[287] However, the agency is responsible for competition and consumer protection across many sectors of the economy. Especially in an era characterized by extreme corporate concentration across multiple sectors, the FTC is already vastly underfunded and understaffed relative to its mandate: As noted previously, over the past four decades, the U.S. economy has nearly tripled while FTC capacity was cut by more than a third.[288] The FTC Office of Technology Research and Investigation has only a handful of staffers to support work across the commission.[289] Adding a large new focus would necessitate a dramatic addition of resources and personnel. In recent history, the FTC also has been more of an enforcement agency than one that engages in rule-making, although it has some ability to do so in cases of demonstrated, prevalent problematic industry practices and where Congress has given it specific ability, as in the Children's Online Privacy Protection Act.

Given the invisible yet pervasive nature of modern digital consumer protections harms and their threats to fundamental rights, the FTC will play a critical role in reigning in predatory practices, regardless of how any other expansions are accomplished.

Expand the FCC: The FCC's roots as a telecommunications regulator tasked with common-carrier oversight suggest some relevance to administering the new online infrastructure model. The agency has significant rule-making expertise and staff technologists who understand the hardware and software sides of core communication technologies and lower-stack internet service providers. The agency may, however, be less well-suited to online services regulation more generally. Its work has historically tended to be deliberate, and it may face challenges in expanding to a broader role charged with competition policy, new technology markets, and dynamic regulation. Therefore, if distributing responsibilities, the more sensible option may be to split administration, housing online infrastructure oversight at the FCC and charging the FTC or a new agency with general online services and gatekeeper oversight.

Expand an existing executive branch agency such as the NTIA or NIST: The National Telecommunications and Information Administration (NTIA) is the executive branch agency charged with advising the president on telecommunications and information policy issues. While industry regulation of this scope and scale have traditionally been outside its mandate, particularly given the FCC's authorities, the NTIA is among the agencies most familiar with internet governance challenges at home and abroad. Similarly, the National Institute of Standards and Technology (NIST) has begun to play a key role in setting cybersecurity standards, analyzing facial recognition, and beginning to outline the impacts of AI. Both the NTIA and NIST are part of the U.S. Department of Commerce, and while they have not historically held robust online services regulation roles, they are clear executive agency candidates for increased involvement. Housing new authorities at the executive agencies does, however, introduce greater risk around politicization and instability that may be precipitated by changes of administration. Thus, expanding the powers of an executive agency—rather than an independent one—would need to overcome steep administrability challenges and require strong congressional oversight.

Establish a new agency: Given the scale of distinctive expertise that effective online services regulation would require, a new agency may be a sensible path forward. A new body offers the chance to think carefully and creatively about administrative design without upending existing work. It enables a fresh start

and dedicated focus, rather than adding a competing one; as Harold Feld notes in his writing on the question, expansion of existing agencies may pit the interests of the new focus against the old, where organizational culture and momentum strongly favor the latter.[290] Other prominent experts and government officials studying the issue have increasingly determined that the challenges of digital markets may require a new entity.[291] Tom Wheeler, the FCC chairman under President Barack Obama, along with Biden administration DOJ antitrust official Gene Kimmelman and former FCC official Phil Verveer, have proposed a new regulatory agency for digital gatekeepers.[292] As a former chairman of the FCC, Wheeler's recommendation for a new agency should be given some weight. Creating a new agency would demand significant resources and political will but may be the better long-term solution for the historic task at hand.

Expand any future new privacy agency: There are several proposals before Congress to create a new federal data privacy agency, similar to the national data protection authorities found in most other countries. These proposals include Sen. Kirsten Gillibrand's (D-NY) Data Protection Act[293] and Reps. Anna Eshoo (D-CA) and Zoe Lofgren's (D-CA) Online Privacy Act.[294] If these bills were enacted and a new data privacy agency established, it may make sense to give the new body a hybrid mandate, to not only tackle privacy issues but also the interlocking economic, civil rights, and consumer protection concerns of the online services industry more broadly. Indeed, privacy is but one among several important areas of work around online services. Policymakers should take care not to solely prioritize privacy at the expense of other critical areas, such as competition, security, and expression.

All of the options outlined above have their advantages and disadvantages, the details of which will be hotly debated as Americans continue to demand action from Congress on tech regulation. Regardless of the chosen future approach, it is clear that the federal government must pursue significant action and investment to regulate online services more effectively, whether through sweeping, comprehensive overhaul or incremental change.

Conclusion

Alongside the many benefits they create, online services have generated widespread economic, consumer, and democratic harms. These harms, however, are not inevitable. Market failures, regulatory gaps, and enforcement oversights have left Americans with few alternatives but to suffer violations of privacy and civil rights in order to use increasingly essential online services.

The evidence of serious problems is clear, yet frustratingly incomplete, as the lack of transparency from online services creates a stark information asymmetry between internet companies and everyone else. The United States lags behind other nations in working to understand and address these harms through regulation, instead ceding immense power over the economy and society entirely to private actors. Unsurprisingly, the individuals and companies that disproportionately benefit from the concentrated economic and political power of online services believe that addressing these harms is heavy-handed. However, the scope, scale, and disproportionate impact of harms from online services on low-income and marginalized communities justify serious action.

Effective online services regulation is essential to creating the future internet that Americans want: one that promotes equitable growth, drives innovation in the public interest, protects freedom of expression, and curbs harms from online services. To achieve this, Congress must prioritize proactive, targeted oversight and dedicated rules and regulation for online services. Together with reinvigorated antitrust action, new competition policy, and robust new federal privacy law or rules, enhanced online services regulation is the critical final tool to reestablish democratic oversight of online services.

In wrangling the universe of online services, this report advanced a three-part framework to address varied challenges. First, it proposed an opt-in online infrastructure tier establishing public interest obligations, including common carriage principles and nondiscrimination, alongside dedicated intermediary liability protections for infrastructural services. Next, the authors outlined the need for dedicated oversight and new, proactive rule-making powers for general online services,

setting up baseline rules for all participants in online services markets based on legislatively enumerated rules and principles. Finally, the authors joined numerous other experts in calling for new tools to reign in the digital gatekeepers that dominate Americans' online lives and address the risks they introduce to national interest, articulating a flexible test to identify gatekeeper services.

There are many potential pathways to actualizing this framework—a combination of new and existing statutes, new rule-making powers, and revived use of existing powers is needed. Likewise, there are several potential strategies for regulatory administration. None of the proposals present a substitute to structural remedies that could more effectively prevent and address inherent conflicts of interest. However, the scope of online issues that are beyond the reach of structural approaches presents a strong argument for additional regulatory capacity. In any arrangement, designing robust safeguards against industry capture is paramount. The Center for American Progress anticipates and welcomes critical conversation on the optimal definitional and administrative approach.

The challenges ahead to U.S. democracy, economy, and society *require* significant investment —and Americans strongly support federal action around online services. A government that cannot understand, much less anticipate, the dangers and potential of new technologies will increasingly fail the public over the coming decades. The road ahead is a significant undertaking, but the cost of inaction would be greater. Better online services are possible, and there is an appropriate role for the U.S. government to play in stewarding that future.

About the authors

Erin Simpson is the associate director of Technology Policy at American Progress, where she develops policy responses to a range of economic, social, and democratic challenges.

Simpson has advocated for platform accountability and improved technology regulation in the European Union, United Kingdom, and United States. Most recently, she served as the civil society lead for the Computational Propaganda Research Project at the Oxford Internet Institute at the University of Oxford, where she supported international civil and human rights leaders in strategic responses to disinformation and democratic resilience.

Simpson's policymaking is informed by her earlier work in civic technology. She was the founding director of programs at Civic Hall Labs, a civic tech research and development nonprofit in New York City, and a Microsoft Civic Tech fellow.

Simpson is a Marshall Scholar and a Truman Scholar. She received two master's degrees from the Oxford Internet Institute at the University of Oxford and earned a bachelor's degree in public policy from the University of Chicago. She is a proud Wisconsinite.

Adam Conner is the vice president for Technology Policy at American Progress. He leads the Technology Policy team as its inaugural vice president, with a focus on building a progressive technology policy platform and agenda.

Conner has spent the past 15 years working at the intersection of technology, politics, policy, and elections as the first Washington, D.C., employee for several Silicon Valley companies. He was a spring 2018 resident fellow at the Harvard University Institute of Politics, where he led a study group titled, "Platforms, Networks, and New Power Technology's Impact on Politics, Policy, and Elections," which focused on the rise of technology companies and their effect on politics and democracy.

Most recently, Conner was the first Washington employee for Slack Technologies, a fast-growing workplace communications startup, leading their engagement with federal, state, and local governments. Prior to that, Conner was vice president of Brigade, a civic engagement startup.

In 2007, Conner founded Facebook's Washington office. He spent seven years on the Facebook privacy and public policy team, where he created the company's government and political outreach efforts and directed their election efforts. His congressional and campaign experience includes the U.S. House Committee on Rules, former Gov. Mark Warner's (D-VA) Forward Together PAC, and John Kerry's 2004 presidential campaign.

Conner is a graduate of George Washington University's School of Media and Public Affairs and serves on the university's board of trustees. He is also on the board of the Roosevelt Institute. He hails from Los Alamos, New Mexico.

Acknowledgments

The authors are grateful to a community of supportive colleagues, friends, and thought partners who shaped this work. They are humbled by and indebted to the critical work of advocates, scholars, and journalists who have persevered against significant odds to illuminate the ways in which online services are changing our lives—for better and for worse. They are deeply grateful to their American Progress colleagues for their support and collaboration, including Ben Olinsky, who was an essential thought partner and supporter in this work, as well as Mara Rudman, Marc Jarsulic, Andres Vinelli, Nicole Ndumele, Simon Clark, Allison Preiss, Peter Gordon, Danielle Root, Todd Phillips, Jarvis Holliday, Irene Koo, Anushree Thekkedath, and Clay Cortez. Special thanks to former CAP President and CEO Neera Tanden for creating the Technology Policy team and giving it the space and encouragement to explore this topic, and current CAP President and CEO Patrick Gaspard for his ongoing support and leadership. The authors are grateful to their partners within the Change the Terms coalition for their tireless and instructive leadership.

The authors wish to additionally thank the following brilliant people who, in their personal capacities, provided time, expertise, and diverse perspectives in the development of this work. The process was iterative, but their patience and wisdom were consistent. The views expressed here, and all errors especially, are the authors' own.

- Yung Au, Oxford Internet Institute
- Rishi Bharwani, Accountable Tech
- John Bergmayer, Public Knowledge
- David Brody, Lawyers' Committee for Civil Rights Under the Law
- Corinne Cath-Speth, Oxford Internet Institute
- Jane Chung, The Worker Agency
- Sara Collins, Public Knowledge
- Harold Feld, Public Knowledge
- Nicole Gill, Accountable Tech
- Greg Guice, Public Knowledge
- Suzanne van Geuns, University of Toronto
- Alex Hart, Freedman Consulting
- Claire Carey, Freedman Consulting
- Jesse Lehrich, Accountable Tech
- Chris Lewis, Public Knowledge
- Chris Murray, Treehouse Solutions
- Corey Owens, Box B Strategies
- Matt Perault, Duke Center on Science and Technology Policy
- Gus Rossi, Omidyar Network
- Ben Scott, Reset
- Kate Sim, Google
- Ganesh Sitaraman, Vanderbilt University
- Charlotte Slaiman, Public Knowledge
- Gigi Sohn, Georgetown Law Institute for Technology Law & Policy and Benton Institute for Broadband & Society
- Kip Wainscott, Stanford Digital Civil Society Lab
- Tom Wheeler, Brookings Institution and Harvard Kennedy School

Endnotes

1 Susannah Fox and Lee Rainie, "The Web at 25 in the U.S. Part 1: How the internet has woven itself into American life," Pew Research Center, February 27, 2014, available at https://www.pewresearch.org/internet/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/.

2 Andrew Perrin and Sara Atske,"About three-in-ten U.S. adults say they are 'almost constantly' online," Pew Research Center, March 26, 2021, available at https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/.

3 Internet Association, "IA Industry Indicators: Data And Analysis for the U.S. Internet Industry, Q1 2020 Data, Q3 2020 Release" (Washington: 2020), available at https://internetassociation.org/publications/ia-industry-indicators-q3-2020/; U.S. Bureau of Economic Analysis, "Updated Digital Economy Estimates – June 2021," available at https://www.bea.gov/data/special-topics/digital-economy (last accessed September 2020).

4 U.S. Census Bureau, "Quarterly Retail E-Commerce Sales: 1st Quarter 2021," Press release, May 18, 2021, available at https://www2.census.gov/retail/releases/historical/ecomm/21q1.pdf.

5 Brooke Auxier and Monica Anderson, "Social Media Use in 2021," Pew Research Center, April 7, 2021, available at https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/; Pew Research Center, "Social Media Fact Sheet," April 7, 2021, available at https://www.pewresearch.org/internet/fact-sheet/social-media/.

6 Elisa Shearer, "More than eight-in-ten Americans get news from digital devices," Pew Research Center, January 12, 2021, available at https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/.

7 Kevin McElrath, "Nearly 93% of Households With School-Age Children Report Some Form of Distance Learning During COVID-19," U.S. Census Bureau, August 26, 2020, available at https://www.census.gov/library/stories/2020/08/schooling-during-the-covid-19-pandemic.html.

8 Kim Parker, Juliana Menasce Horowitz, and Rachel Minkin, "How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work," Pew Research Center, December 9, 2020, available at https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/.

9 Daron Acemoglu and Pascual Restrepo, "Unpacking Skill Bias: Automation and New Tasks," *American Economic Association Papers and Proceedings* 110 (2020): 356, available at https://www.aeaweb.org/articles?id=10.1257/pandp.20201063; Jane G. Gravelle, "Wage Inequality and the Stagnation of Earnings of Low-Wage Workers: Contributing Factors and Policy Options (Washington: Congressional Research Service, 2020), available at https://www.everycrsreport.com/files/20200205_R46212_1f3b076fbd318e142f4cd3e04c4c813cdda1d9a8.pdf; Eduardo Porter, "Tech Is Splitting the U.S. Work Force in Two," *The New York Times*, February 7, 2019, available at https://www.nytimes.com/2019/02/04/business/economy/productivity-inequality-wages.html; Daron Acemoglu, "Breaking up Google and the rest of big tech wouldn't be enough to fix our innovation problems," MarketWatch, November 4, 2020, available at https://www.marketwatch.com/story/breaking-up-google-and-the-rest-of-big-tech-wouldnt-be-enough-to-fix-our-innovation-problems-11604515300; Jonathan P. Allen, *Technology and Inequality: Concentrated Wealth in a Digital World* (New York: Springer, 2017); Zia Qureshi, "Technology, growth, and inequality: Changing dynamics in the digital era" (Washington: Brookings Institution, 2021), available at: https://www.brookings.edu/wp-content/uploads/2021/02/Technology-growth-inequality_final.pdf; Alana Semuels, "Big Tech Is Coming to Small-Town America, But at What Cost?", *Time,* August 24, 2021, available at https://time.com/6085525/big-tech-data-centers/.

10 Charlotte Slaiman, "Data Protection is About Power, Not Just Privacy," Public Knowledge, March 3, 2020, available at https://www.publicknowledge.org/blog/data-protection-is-about-power-not-just-privacy/; Lawyers' Committee for Civil Rights Under Law, "Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce," Press release, August 4, 2021, available at https://www.lawyerscommittee.org/federal-trade-commission-must-protect-civil-rights-privacy-in-online-commerce/.

11 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019).

12 Lawyers' Committee for Civil Rights Under Law and others, "Letter to Chairman Wicker, Chairman Pallone, Ranking Member Cantwell, Ranking Member Walden, and Members of the House and Senate Commerce Committees Re Data-Driven Discrimination and Equal Opportunity in Comprehensive Consumer Privacy Legislation," April 19, 2019, available at https://lawyerscommittee.org/wp-content/uploads/2019/04/Letter-to-Congress-on-Civil-Rights-and-Privacy-4-19-19.pdf.

13 U.S. Federal Trade Commission, "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020," Press release, February 4, 2021, available at https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers. The FTC cites online shopping and internet services in the top five fraud categories. See also Craig Silverman, "These Hugely Popular Android Apps Have Been Committing Ad Fraud Behind Users' Backs," BuzzFeed News, November 16, 2018, available at https://www.buzzfeednews.com/article/craigsilverman/android-apps-cheetah-mobile-kika-kochava-ad-fraud.

14 European Commission, "Impact assessment accompanying the document: Proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services" (Brussels: 2018), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A138%3AFIN; Jerrold Nadler and others, "Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations" (Washington: U.S. House Subcommittee on Antitrust, Commercial and Administrative Law, 2020), available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519; U.S. House Committee on the Judiciary, "AMAZON-HJC-00151722," February 9, 2009, available at https://judiciary.house.gov/uploadedfiles/00151722.pdf.

15 Nadler and others, "Investigation of Competition in Digital Markets"; Marc Jarsulic, "Using Antitrust Law To Address the Market Power of Platform Monopolies" (Washington: Center for American Progress, 2020), available at https://www.americanprogress.org/issues/economy/reports/2020/07/28/488201/using-antitrust-law-address-market-power-platform-monopolies/; Lina M. Khan, "Amazon's Antitrust Paradox," *The Yale Law Journal* 126 (3) (2017): 564–907, available at https://www.yalelawjournal.org/note/amazons-antitrust-paradox.

16 Heidi Ledford, "Millions of Black People Affected by Racial Bias in Health-Care Algorithms," *Nature*, October 24, 2019, available at https://www.nature.com/articles/d41586-019-03228-6; Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018), available at http://algorithmsofoppression.com/.

17 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (New York: Polity, 2019); Umoja Noble, *Algorithms of Oppression*; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018): 1–15, available at https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

18 National Institute of Standards and Technology, "Workshop on Cybersecurity Risks in Consumer Home IoT Products," October 22, 2020, available at https://www.nist.gov/news-events/events/2020/10/workshop-cybersecurity-risks-consumer-home-iot-products.

19 Alexandra Mateescu and Aiha Nguyen, "Explainer: Algorithmic Management in the Workplace" (New York: Data & Society, 2019), available at https://datasociety.net/library/explainer-algorithmic-management-in-the-workplace/.

20 Acemoglu, "Breaking up Google and the rest of big tech wouldn't be enough to fix our innovation problems."

21 Center for an Informed Public and others, "The Long Fuse: Misinformation and the 2020 Election" (Palo Alto, CA: 2021), available at https://purl.stanford.edu/tr171zs0069; Alice E. Marwick, "Why Do People Share Fake News? A Sociotechnical Model of Media Effects," *Georgetown Law Technology Review* (474) (2018), available at https://georgetownlawtechreview.org/why-do-people-share-fake-news-a-sociotechnical-model-of-media-effects/GLTR-07-2018/; Avaaz, "Survivors of Social Media Harm," March 25, 2021, available at https://secure.avaaz.org/campaign/en/facebook_survivors/; Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online" (New York: Data & Society, 2015), available at https://datasociety.net/wp-content/uploads/2017/05/DataAndSociety_MediaManipulationAndDisinformationOnline-1.pdf; Cassie Miller, "White Supremacists See Coronavirus as an Opportunity," Southern Poverty Law Center, March 26, 2020, available at https://www.splcenter.org/hatewatch/2020/03/26/white-supremacists-see-coronavirus-opportunity; Tech Transparency Project, "White Supremacist Groups Are Thriving on Facebook" (Washington: Campaign for Accountability, 2020), available at https://www.techtransparencyproject.org/articles/white-supremacist-groups-are-thriving-on-facebook; Melanie Smith, Erin McAweeney, and Léa Ronzaud, "The COVID-19 'Infodemic': A Preliminary Analysis of the Online Conversation Surrounding the Coronavirus Pandemic" (New York: Graphika, 2020), available at https://public-assets.graphika.com/reports/Graphika_Report_Covid19_Infodemic.pdf.

22 Adam Conner, Erin Simpson, and John Halpin, "Voters Support Enacting Stronger Consumer Protections Online, Antitrust Action for Big Tech Companies," Center for American Progress Action Fund, July 29, 2021, available at https://www.americanprogressaction.org/issues/technology-policy/news/2021/07/29/180584/voters-support-enacting-stronger-consumer-protections-online-antitrust-action-big-tech-companies/; Consumer Reports, "Platform Perceptions: Consumer Attitudes On Competition and Fairness in Online Platforms" (Yonkers, NY: 2020), available at https://advocacy.consumerreports.org/wp-content/uploads/2020/09/FINAL-CR-survey-report.platform-perceptions-consumer-attitudes-.september-2020.pdf.

23 Harold Feld, *The Case for the Digital Platforms Act: Breakups, Starfish Problems, & Tech Regulation* (Washington: Public Knowledge and the Roosevelt Institute, 2019), available at https://www.digitalplatformact.com/; Lina Khan, "The Separation of Platforms and Commerce," *Columbia Law Review* 119 (4) (2019), available at https://columbialawreview.org/content/the-separation-of-platforms-and-commerce/; Tom Wheeler, Phil Verveer, and Gene Kimmelman, "New Digital Realities; New Oversight Solutions" (Cambridge, MA: Harvard Kennedy School Shorenstein Center on Media, Politics, and Public Policy, 2020), available at https://shorensteincenter.org/new-digital-realities-tom-wheeler-phil-verveer-gene-kimmelman/; Fiona M. Scott Morton, "Reforming U.S. antitrust enforcement and competition policy" (Washington: Washington Center for Equitable Growth, 2020), available at http://www.equitablegrowth.org/reforming-u-s-antitrust-enforcement-and-competition-policy/; Gene Kimmelman, "The Right Way to Regulate Digital Platforms," Harvard Kennedy School Shorenstein Center on Media, Politics and Public Policy, September 18, 2019, available at https://shorensteincenter.org/the-right-way-to-regulate-digital-platforms/; K. Sabeel Rahman, "The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept," *Cardozo Law Review* 39 (5) (2018), available at https://papers.ssrn.com/abstract=2986387; Committee on Digital Platforms, "Final Report" (Chicago: University of Chicago Stigler Center for the Study of the Economy and the State, 2019), available at https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf; Tom Wheeler, "A focused federal agency is necessary to oversee big tech" (Washington: Brookings Institution, 2021), available at https://www.brookings.edu/research/a-focused-federal-agency-is-necessary-to-oversee-big-tech/.

24 Khan, "The Separation of Platforms and Commerce"; Khan, "Amazon's Antitrust Paradox"; Zephyr Teachout, *Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money* (New York: St. Martin's Publishing Group, 2020); Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (New York: Columbia Global Reports, 2018); Marc Jarsulic and others, "Reviving Antitrust: Why Our Economy Needs a Progressive Competition Policy" (Washington: Center for American Progress, 2016), available at https://www.americanprogress.org/issues/economy/reports/2016/06/29/140613/reviving-antitrust/.

25 U.K. Competition and Markets Authority, "Online platforms and digital advertising: Market study interim report" (London: 2019), available at https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf; European Commission, "The Digital Services Act package," available at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (last accessed September 2021); Digital Competition Expert Panel, "Unlocking digital competition: Report of the Digital Competition Expert Panel" (London: 2019), available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel; Nadler and others, "Investigation of Competition in Digital Markets"; U.S. House Judiciary Committee, "Chairman Nadler Applauds Committee Passage of Bipartisan Tech Antitrust Legislation," Press release, June 24, 2021, available at https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=4622.

26 U.S. House Judiciary Committee, "Chairman Nadler Applauds Committee Passage of Bipartisan Tech Antitrust Legislation"; Office of Sen. Amy Klobuchar, "Klobuchar, Grassley, Colleagues to Introduce Bipartisan Legislation to Rein in Big Tech," Press release, October 14, 2021, available at https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=3AD365BE-A67E-40BB-908A-C8570FF29600.

27 Consumer Reports and others, "Letter in support of increased funding for the FTC to protect data privacy," September 23, 2021, available at https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf; Electronic Privacy Information Center, "What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities" (Washington: 2021), available at https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.

28 Khan, "The Separation of Platforms and Commerce"; Tim Wu, *The Master Switch* (New York: Alfred A. Knopf, 2010).

29 Ibid. See Part V, D, 3: "A statute from Congress could also establish the principle of separating platforms from commerce—as was the case with banking—with the specific authority to design and implement separations delegated to an agency. This approach would benefit from having an expert agency design and revisit the separation."

30 U.S. Department of the Treasury, "Policy Issues: Designations," available at https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations (last accessed October 2021); Dodd Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, July 21, 2020, available at https://www.govinfo.gov/content/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf.

31 Federal Communications Commission, "In the Matter of Protecting and Promoting the Open Internet," May 15, 2014, available at https://docs.fcc.gov/public/attachments/FCC-14-61A1.pdf.

32 CERN, "World Wide Web," available at http://info.cern.ch/hypertext/WWW/TheProject.html (last accessed September 2021).

33 For a wonderful introduction to layers of the internet and its mapping to the original open systems interconnection model, the authors recommend Ulrike Uhlig and others, *How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship and Governance* (San Francisco: No Starch Press, 2021), pp. 76–77, available at https://nostarch.com/how-internet-really-works#content.

34 Committee on Digital Platforms, "Final Report"; Committee on Digital Platforms, "Market Structure and Antitrust Subcommittee Report."

35 U.K. Office of Communications, "Online market failures and harms: An economic perspective on the challenges and opportunities in regulating online services" (London; 2019), available at https://www.ofcom.org.uk/__data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf.

36 For a discussion of digital market characteristics, see Committee on Digital Platforms, "Final Report"; Committee on Digital Platforms, "Market Structure and Antitrust Subcommittee Report."

37 Ibid.

38 Scholars have been debating the best way to articulate regulation of online services for decades, particularly as they ought to relate to existing telecommunications regulations. For example, see Kevin Werbach, "A Layered Model for Internet Policy," *Journal on Telecommunications & High Technology Law,* 1 (2002): 37, available at http://www.jthtl.org/content/articles/V1I1/JTHTLv1i1_Werbach.PDF.

39 See the disparate impacts in sources throughout the harms section of this report, particularly throughout the subsection titled "Civil rights harms." See additionally U.S. Senate Select Committee on Intelligence, "On Russian Active Measures, Campaigns and Interference in the 2016 U.S Election, Volume 2: Russia's Use of Social Media With Additional Views" (Washington: 2021), available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf; Vera Bergengruen, "Ya Basta. A New Coalition Calls on Facebook to Tackle the Spanish Misinformation Crisis," *Time*, March 16, 2021, available at https://time.com/5947262/spanish-disinformation-facebook/; U.S. Federal Trade Commission, "Consumer Sentinel Network Data Book 2020," available at https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic (last accessed October 2021); U.S. Federal Trade Commission, "Combating Fraud in African American and Latino Communities: The FTC's Comprehensive Strategic Plan" (Washington: 2016), available at https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf; Anti-Defamation League Center for Technology and Society, "Online Hate and Harassment: The American Experience 2021" (New York: March 2021), available at https://www.adl.org/online-hate-2021; Emily A. Vogels, "The State of Online Harassment," Pew Research Center, January 13, 2021, available at https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/; Galen Sherwin and Esha Bhandari, "Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform," American Civil Liberties Union, March 19, 2019, available at https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping; Jinyan Zang, "Solving the problem of racially discriminatory advertising on Facebook" (Washington: Brookings Institution, 2021), available at https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/; Malwarebytes, "Demographics of Cybercrime Report" (Santa Clara, CA: 2021), available at https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html; Ridhi Shetty, "Faster is Not Always Better – Disability Discrimination in Algorithm-driven Hiring Tools" (Washington: Center for Democracy and Technology, 2020), available at https://cdt.org/insights/faster-is-not-always-better-disability-discrimination-in-algorithm-driven-hiring-tools/.

40 A recent letter to the FTC regarding the need to protect civil rights and privacy in online commerce—authored by numerous national advocacy groups, including the Center for American Progress—drew significantly from research and analysis in this section. The letter is available at Lawyers' Committee for Civil Rights Under Law, "Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce."

41 Committee on Digital Platforms, "Market Structure and Antitrust Subcommittee Report."

42 Nadler and others, "Investigation of Competition in Digital Markets"; Committee on Digital Platforms, "Final Report"; *Federal Trade Commission v. Facebook, Inc.*, U.S. District Court for the District of Columbia, No. 1:20-cv-03590-JEB (December 9, 2020), available at https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf; Jarsulic, "Using Antitrust Law To Address the Market Power of Platform Monopolies"; Jarsulic and others, "Reviving Antitrust"; Khan, "Amazon's Antitrust Paradox."

43 Sai Krishna Kamepalli, Raghuram G. Rajan, and Luigi Zingales, "Kill Zone" (Chicago: University of Chicago Becker Friedman Institute for Economics, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555915; Elizabeth Dwoskin, "Facebook's Willingness to Copy Rivals' Apps Seen as Hurting Innovation," *The Washington Post,* August 10, 2017, available at https://www.washingtonpost.com/business/economy/facebooks-willingness-to-copy-rivals-apps-seen-as-hurting-innovation/2017/08/10/ea7188ea-7df6-11e7-a669-b400c5c7e1cc_story.html.

44 Massimo Motta and Martin Peitz, "Big tech mergers," *Information Economics and Policy* (54) (2021): 100868, available at https://www.sciencedirect.com/science/article/abs/pii/S0167624520300111.

45 Colleen Cunningham, Florian Ederer, and Song Ma, "Killer Acquisitions," *Journal of Political Economy* 129 (3) (2021): 649–702, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3241707; The Economist, "American Tech Giants Are Making Life Tough for Startups," June 2018, available at https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups; *Federal Trade Commission v. Facebook, Inc.*, U.S. District Court for the District of Columbia, No. 1:20-cv-03590-JEB (December 9, 2020), available at https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf.

46 Consumer Reports, "Platform Perceptions."

47 Kashmir Hill, "I Cut the 'Big Five' Tech Giants From My Life. It Was Hell," Gizmodo, February 7, 2019, available at https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

48 Tim Wu, "Taking Innovation Seriously: Antitrust Enforcement if Innovation Mattered Most," Antitrust Law Journal 78 (2012): 313, available at https://scholarship.law.columbia.edu/faculty_scholarship/1767/.

49 Karen Hao, "We read the paper that forced Timnit Gebru out of Google. Here's what it says.", *MIT Technology Review,* December 4, 2020, available at https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/; Acemoglu, "Breaking up Google and the rest of big tech wouldn't be enough to fix our innovation problems."

50 Acemoglu, "Breaking up Google and the rest of big tech wouldn't be enough to fix our innovation problems."

51 Ganesh Sitaraman, "The National Security Case for Breaking Up Big Tech" (New York: Knight First Amendment Institute at Columbia University, 2020), available at https://knightcolumbia.org/content/the-national-security-case-for-breaking-up-big-tech.

52 Ashlee Vance, "This Tech Bubble Is Different," *Bloomberg Businessweek*, April 14, 2011, available at https://www.bloomberg.com/news/articles/2011-04-14/this-tech-bubble-is-different?sref=qy93ZUWO

53 Will Oremus, "The Time Jeff Bezos Went Thermonuclear on Diapers.Com," Slate, October 10, 2013, available at https://slate.com/technology/2013/10/amazon-book-how-jeff-bezos-went-thermonuclear-on-diapers-com.html.

54 Nadler and others, "Investigation of Competition in Digital Markets"; U.S. House Committee on the Judiciary, "AMAZON-HJC-00151722."

55 Khan, "Amazon's Antitrust Paradox."

56 See Part I, Section A, in Khan, "The Separation of Platforms and Commerce": "Separate from policies that explicitly or implicitly require merchants and vendors to buy additional Amazon services, sellers worry about subtler forms of discrimination. There are numerous means by which Amazon can disfavor any particular merchant: It can suspend or shut down accounts overnight, withhold merchant funds, change page displays, and throttle or block favorable reviews." See also Leah Nylen and Cristiano Lima, "Big Tech's 'bully' tactics stifle competition, smaller rivals tell Congress," *Politico,* January 17, 2020, available at https://www.politico.com/news/2020/01/17/big-tech-competition-investigation-100701; Emily Stewart, "How big business exploits small business," Vox, June 30, 2021, available at https://www.vox.com/the-goods/22550608/how-big-business-exploits-small-business; Josh Dzieza, "Prime and Punishment: Dirty Dealing in the $175 Billion Amazon Marketplace," The Verge, December 19, 2018, available at https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appeal-reinstatement; Stacy Mitchell, "Amazon Doesn't Just Want to Dominate the Market—It Wants to Become the Market," *The Nation*, February 15, 2018, available at https://www.thenation.com/article/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/.

57 Karen Weise, "Prime Power: How Amazon Squeezes the Businesses Behind Its Store," *The New York Times*, December 19, 2019, available at https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html; Jason Del Rey, "An Amazon revolt could be brewing as the tech giant exerts more control over brands," Vox, November 29, 2018, available at https://www.vox.com/2018/11/29/18023132/amazon-brand-policy-changes-marketplace-control-one-vendor.

58 Tripp Mickle, "Apple Dominates App Store Search Results, Thwarting Competitors," *The Wall Street Journal*, July 23, 2019, available at https://www.wsj.com/articles/apple-dominates-app-store-search-results-thwarting-competitors-11563897221.

59 Spencer Soper, "Amazon Is Accused of Forcing Up Prices in Antitrust Complaint," *Bloomberg,* November 8, 2019, available at https://www.bloomberg.com/news/articles/2019-11-08/amazon-merchant-lays-out-antitrust-case-in-letter-to-congress.

60 Kurt Wagner, "Facebook's Small Advertisers Say They're Hurt by AI Lockouts," *Bloomberg*, December 31, 2021, available at https://www.bloomberg.com/news/articles/2020-12-21/facebook-s-small-advertisers-say-they-re-hurt-by-ai-lockouts.

61 Matthew Prince and Nitin Rao, "AWS's Egregious Egress," The Cloudflare Blog, July 23, 2021, available at https://blog.cloudflare.com/aws-egregious-egress/; Nadler and others "Investigation of Competition in Digital Markets."

62 European Commission, "Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon," Press release, July 17, 2019, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291; Dana Mattioli, "How Amazon Wins: By Steamrolling Rivals and Partners," *The Wall Street Journal,* December 22, 2020, available at https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127; Jack Nicas and Daisuke Wakabayashi, "Sonos, Squeezed by the Tech Giants, Sues Google," *The New York Times*, January 7, 2020, available at https://www.nytimes.com/2020/01/07/technology/sonos-sues-google.html; Aditya Kalra and Steve Stecklow, "Amazon copied products and rigged search results to promote its own brands, documents show," Reuters, October 13, 2021, available at https://www.reuters.com/investigates/special-report/amazon-india-rigging/.

63 European Commission, "Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon," Press release, July 17, 2019, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291; Dana Mattioli, "How Amazon Wins: By Steamrolling Rivals and Partners," *The Wall Street Journal,* December 22, 2020, available at https://www.wsj.com/articles/amazon-competition-shopify-wayfair-allbirds-antitrust-11608235127; Jack Nicas and Daisuke Wakabayashi, "Sonos, Squeezed by the Tech Giants, Sues Google," *The New York Times*, January 7, 2020, available at https://www.nytimes.com/2020/01/07/technology/sonos-sues-google.html; Kalra and Stecklow, "Amazon copied products and rigged search results to promote its own brands, documents show"; Frédéric Lambert and others, "Letter to Commissioner Margrethe Vestager: Google's ongoing abuse of market power is harming consumers and digital companies all over Europe. Comparison shopping services call for vigorous actions against Google's non-compliance with the European Commission's decision in the *Google Search (Shopping)* case," November 28, 2019, available at https://www.hausfeld.com/uploads/documents/final_version_joint_letter_of_css_to_ms_vestager_on_google_shopping-non-compliance_26.11.2019.pdf; Adrianne Jeffries and Leon Yin, "Google's Top Search Result? Surprise! It's Google," The Markup, July 28, 2020, available at https://themarkup.org/google-the-giant/2020/07/28/google-search-results-prioritize-google-products-over-competitors; Mickle, "Apple Dominates App Store Search Results, Thwarting Competitors"; Adrianne Jeffries and Leon Yin, "Amazon Puts Its Own 'Brands' First Above Better-Rated Products," The Markup, October 14, 2021, available at https://themarkup.org/amazons-advantage/2021/10/14/amazon-puts-its-own-brands-first-above-better-rated-products.

64 José Azar, Ioana Marinescu, and Marshall I. Steinbaum, "Labor Market Concentration" (Cambridge, MA: National Bureau of Economic Research, 2019), available at https://www.nber.org/papers/w24147.

65 Council of Economic Advisers, "Labor Market Monopsony: Trends, Consequences, and Policy Responses" (Washington: The White House, 2016), available at https://obamawhitehouse.archives.gov/sites/default/files/page/files/20161025_monopsony_labor_mrkt_cea.pdf.

66 Spencer Soper, "Fired by Bot at Amazon: 'It's You Against the Machine,'" *Bloomberg*, June 28, 2021, available at https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out; Mateescu and Nguyen, "Explainer"; Sam Adler-Bell and Michelle Miller, "The Datafication of Employment: How Surveillance and Capitalism Are Shaping Workers' Futures without Their Knowledge" (New York: The Century Foundation, 2018), available at https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?session=1.

67 American Family Voices, "New Poll Shows Bipartisan Majority Of Americans Want Congress To Rein In Big Tech," Press release, October 13, 2020, available at https://www.prnewswire.com/news-releases/new-poll-shows-bipartisan-majority-of-americans-want-congress-to-rein-in-big-tech-301151327.html.

68 Consumer Reports, "Platform Perceptions."

69 Mark Bergen and Jennifer Surane, "Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales," *Bloomberg*, August 30, 2018, available at https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

70 Justin Brookman, "Understanding the Scope of Data Collection by Major Technology Platforms" (Yonkers, NY: Consumer Reports, 2020), available at https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/05/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf.

71 Jennifer Valentino-DeVries and others, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times*, December 10, 2018, available at https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

72 Daniel Shane, "Facebook collected 1.5 million users' email contacts without their knowledge," CNN Business, April 18, 2019, available at https://www.cnn.com/2019/04/18/business/facebook-email-contacts/index.html; Ryan Nakashima, "Google tracks your movements, like it or not," Associated Press, April 20, 2018, available at https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb.

73 Anne Brunon-Ernst, "The Fallacy of Informed Consent: Linguistic Markers of Assent and Contractual Design in Some E-User Agreements," *Alicante Journal of English Studies* 28 (2015): 37–58, available at https://doi.org/10.14198/raei.2015.28.03; Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* 4 (3) (2008): 543–568, available at https://kb.osu.edu/handle/1811/72839.

74 U.S. Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Press release, July 24, 2019, available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

75 Nick Statt, "Google will fix Chromecast and Google Home bug that reveals a user's location," The Verge, June 18, 2018, available at https://www.theverge.com/2018/6/18/17475766/google-home-chromecast-bug-user-location-reveal.

76 Nakashima, "Google tracks your movements, like it or not."

77 Douglas MacMillan, "Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail," *The Wall Street Journal*, July 2, 2018, available at https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442; James Vincent, "Google wants you to help train its AI by labeling images in Google Photos," The Verge, November 11, 2020, available at https://www.theverge.com/2020/11/11/21559930/google-train-ai-photos-image-labelling-app-android-update; James Vincent, "Yep, human workers are listening to recordings from Google Assistant, too," The Verge, July 11, 2019, https://www.theverge.com/2019/7/11/20690020/google-assistant-home-human-contractors-listening-recordings-vrt-nws.

78 Associated Press, "Facebook reportedly received users' sensitive health data from apps: 'It's incredibly dishonest,'" CBS News, February 22, 2019, available at https://www.cbsnews.com/news/facebook-reportedly-received-sensitive-health-data-from-apps-without-consent/.

79 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, January 18, 2020, available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Valentino-DeVries and others, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret."

80 Howard A. Shelanski, "Information, Innovation, and Competition Policy for the Internet," *University of Pennsylvania Law Review* 161 (2013): 1663–1705, available at https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/6/.

81 Ibid.

82 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 (1) (2019): 39, available at https://lawcat.berkeley.edu/record/1128876?ln=en.

83 Javelin, "Total Identity Fraud Losses Soar to $56 Billion in 2020," Press release, March 23, 2021, available at https://apnews.com/article/science-business-technology-pandemics-public-health-69347fdac-36544cb923022dd3df8d19d; Chris Krebs, "Survey: Americans Spent $1.4B on Credit Freeze Fees in Wake of Equifax Breach," Krebs on Security, March 22, 2018, available at https://krebsonsecurity.com/2018/03/survey-americans-spent-1-4b-on-credit-freeze-fees-in-wake-of-equifax-breach/; Megan Leonhardt, "Consumers lost $56 billion to identity fraud last year—here's what to look out for," CNBC, March 23, 2021, available at https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html.

84 Jonathon W. Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study," *Internet Policy Review* 6 (2) (2017), available at https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case; Jonathon W. Penney, "Whose Speech Is Chilled by Surveillance?", Slate, July 7, 2017, available at https://slate.com/technology/2017/07/women-young-people-experience-the-chilling-effects-of-surveillance-at-higher-rates.html; Alison Snyder, "How surveillance changes behavior," Axios, September 7, 2019, available at https://www.axios.com/surveillance-changes-behavior-36cc1c06-bd2b-4994-8d30-c1b7c274b961.html.

85 Georgetown Law Center on Privacy and Technology, "The Color of Surveillance: Government Monitoring of American Immigrants," June 22, 2017, available at https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/; Our Data Bodies, "Data Justice and Human Rights," available at https://www.odbproject.org/ (last accessed August 2021); Tawana Petty, "Defending Black Lives Means Banning Facial Recognition," Wired, July 10, 2020, available at https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/; Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Face Recognition in America" (Washington: Georgetown University Law School Center on Privacy and Technology, 2016), available at https://www.perpetuallineup.org/; Alvaro M. Bedoya, "Privacy as Civil Right," *New Mexico Law Review* 50 (3) (2020): 301–319, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3599201.

86 Zuboff, "The Age of Surveillance Capitalism."

87 Slaiman, "Data Protection is About Power, Not Just Privacy."

88 Hannah Kuchler, "How Facebook grew too big to handle: The tech giant's 'growth team' brought it over a billion users – but did it also sow the seeds for current troubles?", *Financial Times*, March 28, 2019, available at https://www.ft.com/content/be723754-501c-11e9-9c76-bf4a0ce37d49.

89 Colin Lecher, "How Amazon escapes liability for the riskiest products on its site: Who's at fault when something you buy on Amazon goes bad?", The Verge, January 28, 2020, available at https://www.theverge.com/2020/1/28/21080720/amazon-product-liability-lawsuits-marketplace-damage-third-party.

90 Annie Gilbertson and Jon Keegan, "Amazon's Enforcement Failures Leave Open a Back Door to Banned Goods—Some Sold and Shipped by Amazon Itself," The Markup, June 18, 2020, available at https://themarkup.org/banned-bounty/2020/06/18/amazons-enforcement-failures-leave-open-a-back-door; Alexandra Berzon, Shane Shifflett, and Justin Scheck, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," *The Wall Street Journal*, August 23, 2019, available at https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990; Alexandra Berzon, Justin Scheck, and Shane Shifflett, "Senators Want Answers About Listings for Unsafe Merchandise on Amazon.Com," *The Wall Street Journal*, August 29, 2019, available at https://www.wsj.com/articles/democratic-senators-want-answers-about-listings-for-unsafe-merchandise-on-amazon-com-11567101615.

91 Jon Keegan, "Is This Amazon Review Bullshit?", The Markup, July 21, 2020, available at https://themarkup.org/ask-the-markup/2020/07/21/how-to-spot-fake-amazon-product-reviews; Rob Copeland and Katherine Bindley, "Millions of Business Listings on Google Maps Are Fake—and Google Profits," *The Wall Street Journal*, June 20, 2019, available at https://www.wsj.com/articles/google-maps-littered-with-fake-business-listings-harming-consumers-and-competitors-11561042283; Nicole Nguyen, "Fake Reviews and Inflated Ratings Are Still a Problem for Amazon," *The Wall Street Journal*, June 13, 2021, available at https://www.wsj.com/articles/fake-reviews-and-inflated-ratings-are-still-a-problem-for-amazon-11623587313; Silverman, "These Hugely Popular Android Apps Have Been Committing Ad Fraud Behind Users' Backs"; Greg Bensinger, "Google and Amazon List Gun Accessories for Sale, in Apparent Violation of Their Own Policies," *The Washington Post*, August 6, 2019, available at https://www.washingtonpost.com/technology/2019/08/06/google-amazon-prohibit-firearm-parts-listings-its-easy-find-them-anyway/.

92 Craig Silverman, A.C. Thompson, and Peter Elkind, "Facebook Grew Marketplace to 1 Billion Users. Now Scammers Are Using It to Target People Around the World," ProPublica, September 22, 2021, available at https://www.propublica.org/article/facebook-grew-marketplace-to-1-billion-users-now-scammers-are-using-it-to-target-people-around-the-world; Anna Merlan, "Here Are the Most Common Airbnb Scams Worldwide," Vice, January 31, 2020, available at https://www.vice.com/en/article/epgvm7/airbnb-scam-how-to-tell; Allie Conti, "I Accidentally Uncovered a Nationwide Scam Run by Fake Hosts on Airbnb," Vice, October 31, 2019, available at https://www.vice.com/en/article/43k7z3/nationwide-fake-host-scam-on-airbnb; Silverman, "These Hugely Popular Android Apps Have Been Committing Ad Fraud Behind Users' Backs."

93 Berzon, Shifflett, and Scheck, "Amazon Has Ceded Control of Its Site."

94 Javelin, "Total Identity Fraud Losses Soar to $56 Billion in 2020."

95 Malwarebytes, "Demographics of Cybercrime Report."

96 Committee on Digital Platforms, "Market Structure and Antitrust Subcommittee Report."

97 Forbrukerrådet, "New analysis shows how Facebook and Google push users into sharing personal data," Press release, June 27, 2018, available at https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/; Forbrukerrådet, "You Can Log Out, But You Can Never Leave: How Amazon Manipulates Consumers to Keep Them Subscribed to Amazon Prime," January 14, 2021, available at https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf; Aja Romano, "How Facebook made it impossible to delete Facebook," Vox, March 22, 2018, available at https://www.vox.com/culture/2018/3/22/17146776/delete-facebook-how-to-quit-difficult.

98 Dark Patterns, "Hidden Costs," available at https://www.darkpatterns.org/types-of-dark-pattern/hidden-costs (last accessed September 2021).

99 Consumer Reports, "Collecting #Receipts: Food Delivery Apps & Fee Transparency" (Yonkers, NY: 2020), available at https://digital-lab.consumerreports.org/wp-content/uploads/2021/02/Food-delivery_-Report.pdf.

100 John Brownlee, "After Lawsuit Settlement, LinkedIn's Dishonest Design Is Now A $13 Million Problem," Fast Company, October 5, 2015, available at https://www.fastcompany.com/3051906/after-lawsuit-settlement-linkedins-dishonest-design-is-now-a-13-million-problem.

101 Ryan Calo, "Digital Market Manipulation," *The George Washington Law Review* 82 (2013): 995–1051, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703#.

102 Alfred Ng and Sam Morris, "Dark Patterns that Mislead Consumers Are All Over the Internet," The Markup, June 3, 2021, available at https://themarkup.org/2021/06/03/dark-patterns-that-mislead-consumers-are-all-over-the-internet; Yoree Koh and Jessica Kuronen, "How Tech Giants Get You to Click This (and Not That)," *The Wall Street Journal*, May 31, 2019, available at https://www.wsj.com/articles/how-tech-giants-get-you-to-click-this-and-not-that-11559315900; Jamie Luguri and Lior Jacob Strahilevitz, "Shining a Light on Dark Patterns," *Journal of Legal Analysis* 13 (1) (2021): 43–109, available at https://academic.oup.com/jla/article/13/1/43/6180579; Lauren E. Willis, "Deception by Design" (Los Angeles: Loyola Law School, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694575#.

103 Alex P. Miller and Kartik Hosanagar, "How Targeted Ads and Dynamic Pricing Can Perpetuate Bias," *Harvard Business Review,* November 8, 2019, available at https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias; Giuseppe Dari-Mattiacci and Francesco Parisi, "The Cost of Delegated Control: Vicarious Liability, Secondary Liability and Mandatory Insurance," *International Review of Law and Economics* 23 (4) (2003), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=343120.

104 Consumer Reports, "Platform Perceptions."

105 Akshay Bhargava, "Stalkerware: The Growing Hidden-Software Crisis," *Forbes*, August 28, 2020, available at https://www.forbes.com/sites/forbestechcouncil/2020/08/28/stalkerware-the-growing-hidden-software-crisis/; Molly Dragiewicz and others, "Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms," *Feminist Media Studies* 18 (4) (2018): 609–625, available at https://www.tandfonline.com/doi/full/10.1080/14680777.2018.1447341; Rebecca Lewis, Alice E. Marwick, and William Clyde Partin, "'We Dissect Stupidity and Respond to It': Response Videos and Networked Harassment on YouTube," *American Behavioral Scientist* 65 (5) (2021): 735–756, available at https://journals.sagepub.com/doi/10.1177/0002764221989781; Michael Salter, "From Geek Masculinity to Gamergate: The Technological Rationality of Online Abuse," *Crime Media Culture* 14 (2017), available at https://journals.sagepub.com/doi/10.1177/1741659017690893; Tyler Kingkade and Davey Alba, "A Man Sent 1,000 Men Expecting Sex And Drugs To His Ex-Boyfriend Using Grindr, A Lawsuit Says," BuzzFeed News, January 10, 2019, available at https://www.buzzfeednews.com/article/tylerkingkade/grindr-herrick-lawsuit-230-online-stalking.

106 Knight Foundation and Gallup, "Free Expression, Harmful Speech, and Censorship in a Digital World" (Miami: 2020), available at https://knightfoundation.org/reports/the-future-of-tech-policy-american-views/.

107 Ryan Mac and Tariq Panja, "How Facebook Failed to Stem Racist Abuse of England's Soccer Players," *The New York Times*, August 11, 2021, available at https://www.nytimes.com/2021/08/11/technology/facebook-soccer-racism.html.

108 Victoria Rideout and others, "Coping with COVID-19: How Young People Use Digital Media to Manage Their Mental Health" (San Francisco: Common Sense, Hope Lab, and California Health Care Foundation, 2021), available at https://www.commonsensemedia.org/sites/default/files/uploads/research/2021-coping-with-covid19-full-report.pdf.

109 U.S. Senate Select Committee on Intelligence, "On Russian Active Measures, Campaigns and Interference in the 2016 U.S Election, Volume 2"; Bergengruen, "Ya Basta."; Anti-Defamation League Center for Technology and Society, "Online Hate and Harassment"; Vogels, "The State of Online Harassment"; Shelly Banjo and Bloomberg, "TikTok apologizes after being accused of censoring black users," *Fortune,* July 1, 2020, available at https://fortune.com/2020/06/01/tiktok-apologizes-after-being-accused-of-censoring-black-users/.

110 Dominique Harrison, "Civil Rights Violations in the Face of Technological Change" (Washington: Aspen Institute, 2020), available at https://www.aspeninstitute.org/blog-posts/civil-rights-violations-in-the-face-of-technological-change/; Leadership Conference on Civil and Human Rights and others, "Civil Rights Principles for the Era of Big Data," February 27, 2014, available at https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/#.

111 Gaurav Laroia and David Brody, "Privacy Rights Are Civil Rights. We Need to Protect Them," Free Press, March 14, 2019, available at https://www.freepress.net/our-response/expert-analysis/insights-opinions/privacy-rights-are-civil-rights-we-need-protect-them; Bedoya, "Privacy as Civil Right."

112 Noble, *Algorithms of Oppression*; Buolamwini and Gebru, "Gender Shades"; Cathy O'Neil, *Weapons of Math Destruction* (New York: Penguin Random House, 2017); Danielle Keats Citron and Frank A. Pasquale, "The Scored Society: Due Process for Automated Predictions," *Washington Law Review* 89 (2014), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209; Joy Buolamwini, "How I'm fighting bias in algorithms," TEDxBeaconStreet, March 9, 2017, available at https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms; Mary Madden and others, "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans," *Washington University Law Review* 95 (1) (2017): 53–125, available at https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6265&context=law_lawreview; Sarah Myers West, Meredith Whittaker, and Kate Crawford, "Discriminating Systems: Gender, Race and Power in AI" (New York: AI Now Institute, 2019), available at https://ainowinstitute.org/discriminatingsystems.pdf; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018).

113 Julia Powles, "The Seductive Diversion of 'Solving' Bias in Artificial Intelligence," OneZero, December 7, 2018, available at https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.

114 Miranda Bogen and Aaron Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias" (Washington: Upturn, 2018), available at https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

115 Alina Köchling and Marius Claus Wehner, "Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development," *Business Research* 13 (3) (2020): 795–848, available at https://link.springer.com/article/10.1007/s40685-020-00134-w; Shetty, "Faster is Not Always Better – Disability Discrimination in Algorithm-driven Hiring Tools."

116 Robert Bartlett and others, "Consumer-Lending Discrimination in the FinTech Era" (Cambridge, MA: National Bureau of Economic Research, 2019), available at https://doi.org/10.3386/w25943.

117 Lisa Rice and Deidre Swesnik, "Discriminatory Effects of Credit Scoring on Communities of Color," *Suffolk University Law Review* 46 (3) (2013), available at https://sites.suffolk.edu/lawreview/2013/12/19/discriminatory-effects-of-credit-scoring/.

118 Valerie Schneider, "Locked Out by Big Data: How Big Data, Algorithms, and Machine Learning May Undermine Housing Justice," *Columbia Human Rights Law Review* 52 (1) (2020): 251–305, available at http://hrlr.law.columbia.edu/hrlr/locked-out-by-big-data-how-big-data-algorithms-and-machine-learning-may-undermine-housing-justice/; Emmanuel Martinez and Lauren Kirchner, "The Secret Bias Hidden in Mortgage-Approval Algorithms," The Markup, August 25, 2021, available at https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

119 Hannah Quay-de la Vallee and Natasha Duarte, "Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data" (Washington: Center for Democracy and Technology, 2019), available at https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/; Adam Satariano, "British Grading Debacle Shows Pitfalls of Automating Government," *The New York Times*, August 20, 2020, available at https://www.nytimes.com/2020/08/20/world/europe/uk-england-grading-algorithm.html.

120 Julia Angwin and others, "Machine Bias," ProPublica, May 23, 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=HM_vaeiiqqmnZ9h19EC5CdgRYKiACk6M.

121 Cade Metz and Adam Satariano, "An Algorithm That Grants Freedom, or Takes It Away," *The New York Times*, February 6, 2020, available at https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html.

122 Ziad Obermeyer and others, "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366 (6464) (2019): 447–453, available at https://doi.org/10.1126/science.aax2342; Ledford, "Millions of Black People Affected by Racial Bias in Health-Care Algorithms."

123 Galen Sherwin and Esha Bhandari, "HUD Is Reviewing Twitter's and Google's Ad Practices as Part of Housing Discrimination Probe," *The Washington Post*, March 19, 2019, available at https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/.

124 For a more detailed survey of harms relating to algorithmic racism, see Jane Chung, "Racism In, Racism Out: A Primer on Algorithmic Racism" (Washington: Public Citizen, 2021), available at https://www.citizen.org/article/algorithmic-racism/.

125 Margaret Hu, "Algorithmic Jim Crow," *Fordham Law Review* 86 (2) (2017): 633–696, available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=5445&context=flr; Yeshimabeit Milner and Amy Traub, "Data Capitalism and Algorithmic Racism" (New York: Data for Black Lives and Demos, 2021), available at https://www.demos.org/research/data-capitalism-and-algorithmic-racism; Benjamin, *Race After Technology*

; Chung, "Racism In, Racism Out."

126 Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information

Civilization," *Journal of Information Technology* 30 (1) (2015): 75–89, available at https://journals.sagepub.com/doi/10.1057/jit.2015.5; Tressie McMillan Cottom, "Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society," *Sociology of Race and Ethnicity* 6 (4) (2020): 441–449, available at https://journals.sagepub.com/doi/pdf/10.1177/2332649220949473; Milner and Traub, "Data Capitalism and Algorithmic Racism."

127 Joseph Blass, "Algorithmic Advertising Discrimination," *Northwestern University Law Review* 114 (2) (2019), available at https://scholarlycommons.law.northwestern.edu/nulr/vol114/iss2/3; Adler-Bell and Miller, "The Datafication of Employment."

128 Galen Sherwin and Esha Bhandari, "Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform," American Civil Liberties Union, March 19, 2019, available at https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping; Katie Benner, Glenn Thrush and Mike Isaac, "Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says," *The New York Times,* March 28, 2019, available at https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html.

129 Keats Citron and Pasquale, "The Scored Society"; Solon Barocas and Andrew D. Selbst, "Big Data's Disparte Impact," *California Law Review* 104 (671) (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899; Milner and Traub, "Data Capitalism and Algorithmic Racism."

130 Shetty, "Faster is Not Always Better – Disability Discrimination in Algorithm-driven Hiring Tools."

131 Benjamin Edelman, Michael Luca, and Dan Svirsky, "Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment," *American Economic Journal: Applied Economics* 9 (2) (2017): 1–22, available at https://doi.org/10.1257/app.20160213; Yanbo Ge and others, "Racial and Gender Discrimination in Transportation Network Companies" (Cambridge, MA: National Bureau of Economic Research, 2016), available at https://www.nber.org/papers/w22776; Alex Rosenblat and others, "Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination," *Policy & Internet* 9 (3) (2017): 256–279, available at https://doi.org/10.1002/poi3.153.

132 Center for Democracy Technology and others, "Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology," June 3, 2021, available at https://cdt.org/wp-content/uploads/2021/06/2021-06-03-CDT-OTI-Upturn-TLC-FINAL-Civil-Rights-Statement-of-Concerns.pdf.

133 Buolamwini and Gebru, "Gender Shades."

134 Garvie, Bedoya, and Frankle, "The Perpetual Line Up."

135 Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times*, December 29, 2020, available at https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

136 Rebecca Lewis, "Alternative Influence: Broadcasting the Reactionary Right on YouTube" (New York: Data and Society, 2018), available at https://datasociety.net/library/alternative-influence/; Manoel Horta Ribeiro and others, "Auditing Radicalization Pathways on YouTube" (Barcelona, Spain: 2020), available at https://dl.acm.org/doi/10.1145/3351095.3372879; Jeff Horwitz and Deepa Seetharaman, "Facebook Executives Shut Down Efforts to Make the Site Less Divisive," *The Wall Street Journal*, May 26, 2020, available at https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

137 Canadian Centre for Child Protection, "Resources and Research: Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms," available at https://protectchildren.ca/en/resources-research/csam-reporting-platforms/ (last accessed August 2021); J. Nathan Matias and others, "Reporting, Reviewing, and Responding to Harassment on Twitter" (Ithaca, NY: Women, Action, and the Media, 2015), available at https://arxiv.org/abs/1505.03359v1.

138 Ian Vandewalker, "Digital Disinformation and Vote Suppression" (New York: Brennan Center for Justice, 2020), available at https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression.

139 Kristen Clarke and David Brody, "It's Time for an Online Civil Rights Act," The Hill, August 3, 2018, available at https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act.

140 Kevin Roose, "Social Media Giants Support Racial Justice. Their Products Undermine It," *The New York Times*, June 19, 2020, available at https://www.nytimes.com/2020/06/19/technology/facebook-youtube-twitter-black-lives-matter.html.

141 Noble, "Algorithms of Oppression."

142 Latanya Sweeney, "Discrimination in Online Ad Delivery" (Cambridge, MA: Social Science Research Network, 2013), available at https://doi.org/10.2139/ssrn.2208240.

143 Paul Baker and Amanda Potts, "'Why do white people have thin lips?' Google and the perpetuation of stereotypes via auto-complete search forms," *Critical Discourse Studies* 10 (2) (2013): 187–204, available at https://doi.org/10.1080/17405904.2012.744320; Issie Lapowsky, "Google Autocomplete Still Makes Vile Suggestions," Wired, February 12, 2018, available at https://www.wired.com/story/google-autocomplete-vile-suggestions/; Moin Nadeem, Anna Bethke, and Siva Reddy, "StereoSet: Measuring stereotypical bias in pretrained language models" (Ithaca, NY: 2020), available at http://arxiv.org/abs/2004.09456.

144 Allison Koenecke and others, "Racial Disparities in Automated Speech Recognition," *Proceedings of the National Academy of Sciences* 117 (14) (2020): 7684–7689, available at https://doi.org/10.1073/pnas.1915768117; Tom Simonite, "When It Comes to Gorillas, Google Photos Remains Blind," Wired, January 11, 2018, available at https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/; Buolamwini and Gebru, "Gender Shades."

145 Elizabeth L. Eisenstein, *The Printing Revolution in Early Modern Europe* (Cambridge, UK: Cambridge University Press, 2012), available at https://doi.org/10.1017/CBO9781139197038; Tom Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers* (New York: Bloomsbury Publishing, 2014), available at https://www.bloomsbury.com/us/victorian-internet-9781620405925.

146 Nancy Zdunkewicz and Change Research, "Strong bipartisan support for regulation of tech & social media," Memo, July 29, 2021, available at https://cdn.americanprogressaction.org/content/uploads/sites/2/2021/07/28065416/Tech-Policy-Polling-Memo_7.29.21_Change-Research.pdf.

147 Jarsulic and others, "Reviving Antitrust."

148 Marc Jarsulic, Ethan Gurwitz, and Andrew Schwartz, "Toward a Robust Competition Policy" (Washington: Center for American Progress, 2019), available at https://www.americanprogress.org/issues/economy/reports/2019/04/03/467613/toward-robust-competition-policy/.

149 Lawyers' Committee for Civil Rights Under Law, "Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce," Press release, August 4, 2021, available at https://www.lawyerscommittee.org/federal-trade-commission-must-protect-civil-rights-privacy-in-online-commerce/.

150 Consumer Reports and others, "Letter in support of increased funding for the FTC to protect data privacy."

151 Public Citizen, "58 Groups Urge Swift Passage of House Bills to Break Up Big Tech," Press release September 2, 2021, available at https://www.citizen.org/news/58-groups-urge-swift-passage-of-house-bills-to-break-up-big-tech/.

152 Office of Sen. Amy Klobuchar, "Support Builds for Bipartisan Legislation From Klobuchar, Grassley, and Colleagues to Rein in Big Tech," Press release, October 18, 2021, available at https://www.klobuchar.senate.gov/public/index.cfm/2021/10/support-builds-for-bipartisan-legislation-from-klobuchar-grassley-and-colleagues-to-rein-in-big-tech.

153 Consumer Reports and others, "Letter in support of increased funding for the FTC to protect data privacy."

154 Nadler and others, "Investigation of Competition in Digital Markets."

155 U.S. Federal Trade Commission, "Guide to Antitrust Laws: The Antitrust Laws," available at https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws (last accessed October 2021).

156 John M. Newman, "Antitrust in Digital Markets," *Vanderbilt Law Review* 72 (5) (2019), available at https://scholarship.law.vanderbilt.edu/vlr/vol72/iss5/2/.

157 Jarsulic and others, "Reviving Antitrust."

158 U.S. Department of Justice, Office of Public Affairs, "Justice Department Sues Monopolist Google For Violating Antitrust Laws: Department Files Complaint Against Google to Restore Competition in Search and Search Advertising Markets," Press release, October 20, 2020, available at https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws; John D. McKinnon and Ryan Tracy, "Ten States Sue Google, Alleging Deal With Facebook to Rig Online Ad Market," *The Wall Street Journal*, December 16, 2020, available at https://www.wsj.com/articles/states-sue-google-over-digital-ad-practices-11608146817; U.S. Department of Justice, "Justice Department Files Lawsuit Against Facebook for Discriminating Against U.S. Workers: Lawsuit Alleges Facebook Favors H-1B Visa Workers and Other Temporary Visa Holders over U.S. Workers," Press release, December 3, 2020, available at https://www.justice.gov/opa/pr/justice-department-files-lawsuit-against-facebook-discriminating-against-us-workers; U.S. Federal Trade Commission, "FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate," Press release, August 19, 2021, available at https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush.

159 Andrew Ross Sorkin and others, "Apple's Shrewd App Store Settlement," *The New York Times,* August 27, 2021, available at https://www.nytimes.com/2021/08/27/business/dealbook/apple-app-store-lawsuits.html.

160 Stephen Nellis and Tim Kelly, "Apple offers small concession in easing App Store rules for Netflix, others," Reuters, September 2, 2021, available at https://www.reuters.com/technology/apple-says-japan-fair-trade-commission-closes-app-store-investigation-2021-09-02/.

161 Jarsulic, Gurwitz, and Schwartz, "Toward a Robust Competition Policy"; "Executive Order on Promoting Competition in the American Economy," The White House, Press release, July 9, 2021, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

162 Nadler and others, "Investigation of Competition in Digital Markets."

163 Ibid.

164 U.S. House Committee on the Judiciary, "House Lawmakers Release Anti-Monopoly Agenda for 'A Stronger Online Economy: Opportunity, Innovation, Choice,'" Press release, June 11, 2021, available at https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=4591.

165 American Choice and Innovation Online Act, H.R. 3816, 117th Cong., 1st sess. (June 11, 2021), available at https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/American%20Innovation%20and%20Choice%20Online%20Act%20-%20Bill%20Text.pdf.

166 Platform Competition and Opportunity Act, H.R. 3826, 117th Cong., 1st sess. (June 11, 2021), available at https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/Platform%20Competition%20and%20Opportunity%20Act%20-%20Bill%20Text%20%281%29.pdf.

167 Augmenting Compatibility and Competition by Enabling Service Switching Act, H.R. 3849, 117th Cong., 1st sess. (June 11, 2021), available at https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/ACCESS%20Act%20-%20Bill%20Text%20%281%29.pdf.

168 Merger Filing Fee Modernization Act, H.R. 3843, 117th Cong., 1st sess. (June 11, 2021), available at https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/Merger%20Filing%20Fee%20Modernization%20Act%20of%202021%20-%20Bill%20Text%20%281%29.pdf.

169 State Antitrust Enforcement Venue Act, H.R. 3460, 117th Cong., 1st sess. (June 11, 2021), available at https://buck.house.gov/sites/buck.house.gov/files/H.R.%203460%20-%20The%20State%20Antitrust%20Enforcement%20Venue%20Act%20of%202021.pdf.

170 Ending Platform Monopolies Act, H.R. 3825, 117th Cong., 1st sess. (June 11, 2021), available at https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/Ending%20Platform%20Monopolies%20-%20Bill%20Text.pdf.

171 American Choice and Innovation Online Act, H.R. 3816.

172 Office of Sen. Amy Klobuchar, "Support Builds for Bipartisan Legislation From Klobuchar, Grassley, and Colleagues to Rein in Big Tech."

173 Better Online Ticket Sales Act, 15 U.S.C. § 45c, available at http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section45c&num=0&edition=prelim (last accessed October 2021).

174 Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, available at http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim (last accessed October 2021).

175 Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401-8405, available at https://www.ftc.gov/enforcement/statutes/restore-online-shoppers-confidence-act (last accessed October 2021).

176 U.S. Federal Trade Commission, "What We Do," available at https://www.ftc.gov/about-ftc/what-we-do (last accessed August 2021).

177 Carolyn Carter, "Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws," (Boston: National Consumer Law Center, 2018), available at https://www.nclc.org/images/pdf/udap/udap-report.pdf.

178 Rohit Chopra, "Statement of Commissioner Rohit Chopra Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security," U.S. Federal Trade Commission, June 18, 2020, available at https://www.ftc.gov/public-statements/2020/06/statement-commissioner-rohit-chopra-regarding-report-congress-ftcs-use-its.

179 Ibid. See also Cecilia Kang, "Here's How the Telecom Industry Plans to Defang Their Regulators," *The Washington Post*, September 12, 2013, available at https://www.washingtonpost.com/news/the-switch/wp/2013/09/12/heres-how-the-telecom-industry-plans-to-defang-their-regulators/.

180 Consumer Reports and others, "Letter to House and Senate Leadership from civil rights, civil liberties, and consumer protection organizations in support of increased FTC funding in the Build Back Better Act," September 23, 2021, available at https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf; U.S. Federal Trade Commission, "FTC Appropriation and Full-Time Equivalent (FTC) History," available at https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation (last accessed April 2021).

181 Ibid.

182 U.S. Federal Trade Commission, "Privacy and Security Enforcement," available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last accessed September 2021).

183 Rebecca Kelly Slaughter, "FTC Data Privacy Enforcement: A Time of Change: Remarks at the Cybersecurity and Data Privacy Conference Program on Corporate Compliance and Enforcement, New York University School of Law," October 16, 2020, available at https://www.ftc.gov/system/files/documents/public_statements/1581786/slaughter_-_remarks_on_ftc_data_privacy_enforcement_-_a_time_of_change.pdf.

184 U.S. Federal Trade Commission, "FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security" (Washington: 2020), available at https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf.

185 European Data Protection Board, "Our Members," available at https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-EDPS (last accessed September 2021).

186 See Christine Bannan and Raj Gambhir, "Does Data Privacy Need Its Own Agency?" (Washington: New America Open Technology Institute, 2021), available at http://newamerica.org/oti/reports/does-data-privacy-need-its-own-agency/, for specific comparison with the Irish Data Protection Authority and related discussion of whether a dedicated agency is needed for privacy regulation.

187 Mark Scott, "EU privacy enforcer hits make-or-break moment: Ireland's Data Protection Commission is under pressure to act soon," *Politico EU*, May 21, 2020, available at https://www.politico.eu/article/data-protection-privacy-ireland-helen-dixon-gdpr/.

188 California Legislative Information, "Title 1.81.5. Consumer Privacy Act of 2018," available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (last accessed September 2021); California Privacy Rights Act of 2020, "Proposition 24," available at https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf (last accessed September 2021).

189 Virginia Legislative Information Session, "SB 1392 Consumer Data Protection Act of 2021; establishes a framework for controlling and processing personal data," available at https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392 (last accessed September 2021); Colorado General Assembly, "SB21-190 Protect Personal Data Privacy of 2021," available at https://leg.colorado.gov/bills/sb21-190 (last accessed September 2021).

190 Consumer Federation of California Education Foundation, "California Online Privacy Protection Act (CalOPPA)," available at https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/ (last accessed September 2021).

191 Robert Gellman, "Can Consumers Trust the FTC to Protect Their Privacy?", American Civil Liberties Union, October 25, 2016, available at https://www.aclu.org/blog/privacy-technology/internet-privacy/can-consumers-trust-ftc-protect-their-privacy.

192 Bannan and Gambhir, "Does Data Privacy Need Its Own Agency?"

193 Electronic Privacy Information Center, "What the FTC Could Be Doing (But Isn't) To Protect Privacy."

194 Slaughter, "FTC Data Privacy Enforcement: A Time of Change: Remarks at the Cybersecurity and Data Privacy Conference Program on Corporate Compliance and Enforcement, New York University School of Law." For more on Magnuson Moss rule-making, see U.S. Federal Trade Commission, "Magnuson Moss Warranty-Federal Trade Commission Improvements Act," available at https://www.ftc.gov/enforcement/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act (last accessed September 2021).

195 Leah Nylen, "'Unlike anything I've seen at the FTC': Biden's chair makes her public debut," *Politico*, July 1, 2021, available at https://www.politico.com/news/2021/07/01/ftc-lina-khan-antitrust-chair-497764.

196 John D. McKinnon and Ryan Tracy, "FTC Weighs New Online Privacy Rules," *The Wall Street Journal,* September 29, 2021, available at https://www.wsj.com/articles/ftc-weighs-new-online-privacy-rules-11632913200.

197 Benjamin Din, "House E&C seeks major boost to FTC privacy efforts," *Politico*, September 13, 2021, available at https://www.politico.com/newsletters/morning-tech/2021/09/13/house-e-c-seeks-major-boost-to-ftc-privacy-efforts-797555.

198 SAFE DATA Act, S. 4626, 116th Cong., 1st sess. (September 17, 2020), available at https://www.congress.gov/bill/116th-congress/senate-bill/4626/text; Consumer Online Privacy Rights Act, S. 2968, 116th Cong., 1st sess. (December 3, 2019), available at https://www.congress.gov/bill/116th-congress/senate-bill/2968/text; Online Privacy Act, H.R. 4978, 116th Cong., 1st sess. (November 4, 2019), available at https://www.congress.gov/bill/116th-congress/house-bill/4978/text.

199 Data Protection Act, S. 2134, 117th Cong., 1st sess. (June 17, 2021), available at https://www.congress.gov/bill/117th-congress/senate-bill/2134/text.

200 Din, "House E&C seeks major boost to FTC privacy efforts"; Build Back Better Act, H.R. 5376, 117th Cong., 1st sess. (November 3, 2021), available at https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR5376RH-RCP117-18.pdf.

201 Accountable Tech, "Ban Surveillance Advertising," available at https://accountabletech.org/campaign/ban-surveillance-advertising/ (last accessed September 2021).

202 Sam Sabin, "Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year," Morning Consult, December 18, 2019, available at https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/.

203 Lawyers' Committee for Civil Rights Under Law and others, "Re: Protecting civil rights and privacy," Chair Lina Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson, August 2021, available at https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.

204 Talia B. Gillis and Jann L. Spiess, "Big Data and Discrimination," *University of Chicago Law Review* 86 (2) 2019), available at https://chicagounbound.uchicago.edu/uclrev/vol86/iss2/4/.

205 Robyn Caplan and others, "Algorithmic Accountability: A Primer" (New York: Data and Society, 2018), available at https://datasociety.net/library/algorithmic-accountability-a-primer/.

206 Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR," *Harvard Journal of Law & Technology* 31 (2018): 841–887, available at https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf.

207 Meta, "Introducing Meta: A Social Technology Company," Press release, October 28, 2021, available at https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

208 Jarsulic, "Using Antitrust Law To Address the Market Power of Platform Monopolies."

209 U.S. Federal Trade Commission, "FTC Sues Facebook for Illegal Monopolization: Agency challenges Facebook's multi-year course of unlawful conduct," Press release, December 9, 2020, available at https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization.

210 Salvador Rodriguez, "Judge dismisses FTC and state antitrust complaints against Facebook," CNBC, June 28, 2021, available at https://www.cnbc.com/2021/06/28/judge-dismisses-ftc-antitrust-complaint-against-facebook.html.

211 Cecilia Kang, "U.S. Revives Facebook Suit, Adding Details to Back Claim of a Monopoly," *The New York Times*, August 19, 2021, available at https://www.nytimes.com/2021/08/19/technology/ftc-facebook-antitrust.html.

212 Facebook, Inc., "Facebook Reports Second Quarter 2021 Results," Press release, July 28, 2021, available at https://s21.q4cdn.com/399680738/files/doc_financials/2021/q2/FB-06.30.2021-Exhibit-99.1_final.pdf; *Federal Trade Commission v. Facebook, Inc.*, U.S. District Court for the District of Columbia, No. 1:20-cv-03590-JEB (December 9, 2020), available at https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf.

213 Feld, *The Case for the Digital Platforms Act: Breakups, Starfish Problems, & Tech Regulation*.

214 Joe Mandese, "Facebook Ad Products Chief: Context Will Be More Of Our King," MediaPost, July 8, 2021, available at https://www.mediapost.com/publications/article/364902/facebook-ad-products-chief-context-will-be-more-o.html.

215 Zang, "Solving the problem of racially discriminatory advertising on Facebook"; American Civil Liberties Union, "Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform;" Laura W. Murphy, Megan Cacace, and others, "Facebook's Civil Rights Audit – Final Report," July 2020, available at https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf.

216 An example of this approach can be seen in the bipartisan American Innovation and Choice Online Act, introduced by Sens. Amy Klobuchar (D-MN) and Chuck Grassley (R-IA) and Reps. David Cicilline (D-RI) and Lance Gooden (R-TX), which sets out clear restrictions against certain kinds of anti-competitive behavior by dominant online platforms instead of relying on existing ex post litigation under the Sherman or Clayton Acts.

217 Rebecca Kelly Slaughter, "Prepared Statement of Federal Trade Commission Acting Chairwoman Rebecca Kelly Slaughter Before the Subcommittee on Antitrust, Commercial and Administrative Law Of the Judiciary Committee, United States House of Representatives, Reviving Competition, Part 3: Strengthening the Laws to Address Monopoly Power," March 18, 2021 available at https://www.ftc.gov/system/files/documents/public_statements/1588320/p180101_prepared_statement_of_ftc_acting_chairwoman_slaughter.pdf.

218 Feld, *The Case for the Digital Platforms Act: Breakups, Starfish Problems, & Tech Regulation*, pp. 31–32.

219 Associated Press, "Swaths Of The Internet Go Down After Cloud Outage," NPR, June 8, 2021, available at https://www.npr.org/2021/06/08/1004305569/internet-fastly-outage-go-down-twitter-reddit; Corinne Cath-Speth, @C___CS, June 8, 2021, 7:23 a.m. ET, Twitter, available at: https://twitter.com/C___CS/status/1402224707366227972; Laura DeNardis, "Facebook's global outage wasn't the result of a hack, but big political questions lurk behind it," *The Washington Post,* October 8, 2021, available at https://www.washingtonpost.com/politics/2021/10/08/facebooks-global-outage-wasnt-result-hack-big-political-questions-lurk-behind-it/.

220 Federal Communications Commission, "In the Matter of Protecting and Promoting the Open Internet: GN Docket No. 14-28," May 15, 2014, available at https://docs.fcc.gov/public/attachments/FCC-14-61A1.pdf, p. 4.

221 For a synthesis of this history, see "A History of Layer-Conscious Internet Regulation" in Annemarie Bridy, "Remediating Social Media: A Layer-Conscious Approach," *Boston University Journal of Science and Technology Law* 24 (2018): 193, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3154117.

222 Prince and Rao, "AWS's Egregious Egress."

223 Nicola Jones, "How to stop data centres from gobbling up the world's electricity," *Nature,* September 12, 2018, available at https://www.nature.com/articles/d41586-018-06610-y; Olivia Solon, "Drought-stricken communities push back against data centers," NBC News, June 19, 2021, available at https://www.nbcnews.com/tech/internet/drought-stricken-communities-push-back-against-data-centers-n1271344; Bianca Bosker, "Why Everything is Getting Louder," *The Atlantic*, November 2019, available at https://www.theatlantic.com/magazine/archive/2019/11/the-end-of-silence/598366/; U.S. Department of Energy Office of Energy Efficiency and Renewable Energy, "Data Centers and Servers," available at https://www.energy.gov/eere/buildings/data-centers-and-servers (last accessed November 2021).

224 Solon, "Drought-stricken communities push back against data centers."

225 Change the Terms, "Reducing Hate Online," available at https://www.changetheterms.org/ (last accessed July 2020); SantaClaraPrinciples.org, "The Santa Clara Principles on Transparency & Accountability in Content Moderation," available at https://santaclara-principles.org/images/scp-og.png (last accessed November 2021).

226 Suzanne van Geuns and Corinne Cath-Speth, "How Hate Speech Reveals the Invisible Politics of Internet Infrastructure," Brookings TechStream, August 20, 2020, available at https://www.brookings.edu/techstream/how-hate-speech-reveals-the-invisible-politics-of-internet-infrastructure/; Jack M. Balkin, "Free Speech Is a Triangle," *Columbia Law Review* 118 (7) (2018), available at https://columbialawreview.org/content/free-speech-is-a-triangle/; Daphne Keller, "Who Do You Sue? State and Platform Hybrid Power Over Online Speech" (Palo Alto, CA: Hoover Institution at Stanford University, 2019), available at https://www.hoover.org/research/who-do-you-sue; Annemarie Birdy, "Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation," *Washington and Lee Law Review* 74 (2017): 1345–1388, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920805; Brenden Kuerbis, Ishan Mehta, and Milton Mueller, "In Search of Amoral Registrars: Content Regulation and Domain Name Policy" (Atlanta: Georgia Institute of Technology Internet Governance Project, 2017), available at https://www.internetgovernance.org/wp-content/uploads/AmoralReg-PAPER-final.pdf; Joan Donovan, "Navigating the Tech Stack: When, Where and How Should We Moderate Content?", Centre for International Governance Innovation, October 28, 2019, available at https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content/; Ben Thompson, "Moderation in Infrastructure," Stratechery, March 16, 2021, available at https://stratechery.com/2021/moderation-in-infrastructure/. Regarding human rights implications specifically, see Article 19, "Digital freedom: Building an Internet infrastructure that protects human rights," June 8, 2021, available at https://www.article19.org/resources/digital-freedom-building-an-internet-infrastructure-that-protects-human-rights/; Monika Zalnieriute and Stefania Milan, "Internet Architecture and Human Rights: Beyond the Human Rights Gap," *Policy & Internet* 11 (1) (2019), available at https://onlinelibrary.wiley.com/doi/10.1002/poi3.200.

227 Balkin, "Free Speech Is a Triangle."

228 Ibid.; Laura DeNardis and Andrea Hackl, "Internet control points as LGBT rights mediation," *Information, Communication, and Society* (19) (2016), available at https://www.tandfonline.com/doi/abs/10.1080/1369118X.2016.1153123; Emma Llanso, "OnlyFans Isn't The First Site To Face Moderation Pressure From Financial Intermediaries, And It Won't Be The Last," TechDirt, October 5, 2021, available at https://www.techdirt.com/articles/20211005/11512347706/onlyfans-isnt-first-site-to-face-moderation-pressure-financial-intermediaries-it-wont-be-last.shtml.

229 Annie Palmer, "Amazon says it's been flagging violent posts to Parler since November," CNBC, January 13, 2021, available at https://www.cnbc.com/2021/01/13/amazon-says-violent-posts-forced-it-to-drop-parler-from-its-web-hosting-service.html; José Van Dijck, Tim de Winkel, and Mirko Tobias Schäfer, "Deplatformization and the governance of the platform ecosystem," *New Media & Society* (2021), available at https://journals.sagepub.com/doi/pdf/10.1177/14614448211045662.

230 Casey Newton, "Everything You Need to Know About Section 230: The most important law for online speech," The Verge, December 29, 2020, available at https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation.

231 Corinne Reichert, "Trump vetoes defense bill over Congress' refusal to repeal Section 230," CNET, December 23, 2020, available at https://www.cnet.com/tech/mobile/trump-vetoes-defense-bill-over-congress-refusal-to-repeal-section-230/; Editorial Board, "Opinion: Joe Biden, Former vice president of the United States," *The New York Times*, January 17, 2021, available at https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html?smid=nytcore-ios-share.

232 Indeed, the Platform Accountability and Consumer Transparency Act from Sens. Brian Schatz (D-HI) and John Thune (R-SD) and the Protecting Americans from Dangerous Algorithms Act from Reps. Tom Malinowski (D-NJ) and Anna Eshoo (D-CA) specifically exempt internet infrastructure. The Justice Against Malicious Algorithms Act of 2021 introduced by leading House Democrats in October 2021 further attempts to exempt internet infrastructure from proposed changes to Section 230 by defining it as "a provider of an interactive computer service to the extent that the service, system, or access software of such provider is used by another interactive computer service for the management, control, or operation of such other interactive computer service" and specifically identifying web hosting, domain registration, content delivery networks, caching, data storage, and cybersecurity.

233 Jonathan Zittrain, The Inexorable Push For Infrastructure Moderation," TechDirt, September 24, 2021, available at https://www.techdirt.com/articles/20210924/12012347622/inexorable-push-infrastructure-moderation.shtml.

234 Reps. Katie Porter and Representative Nydia Velázquez, "Letter to Honorable Steven T. Mnuchin to consider designating cloud-storage providers as SIFMUs," August 22, 2019, available at https://velazquez.house.gov/sites/velazquez.house.gov/files/FSOC%20cloud%20.pdf.

235 National Center for Missing & Exploited Children, "Child Sexual Abuse Material (CSAM)," available at https://www.missingkids.org/theissues/csam (last accessed October 2021).

236 U.S. Department of State, "Foreign Terrorist Organizations," available at https://www.state.gov/foreign-terrorist-organizations (last accessed October 2021).

237 U.S. Department of Treasury, "Sanctions Programs and Country Information," available at https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information (last accessed October 2021).

238 Jones, "How to stop data centres from gobbling up the world's electricity."

239 European Digital Media Observatory, "Call for Comment on GDPR Article 40 Working Group," Press release, November 24, 2020, available at https://edmo.eu/2020/11/24/call-for-comment-on-gdpr-article-40-working-group/.

240 Alex Engler, "Platform data access is a lynchpin of the EU's Digital Services Act," Brookings Institution, January 15, 2021, available at https://www.brookings.edu/blog/techtank/2021/01/15/platform-data-access-is-a-lynchpin-of-the-eus-digital-services-act/.

241 Social Media DATA Act of 2021, H.R. 3451, 117th Cong., 1st sess. (May 20, 2021), available at https://www.congress.gov/bill/117th-congress/house-bill/3451.

242 U.S. Department of Transportation and National Science and Technology Council, "Ensuring American Leadership in Automated Vehicle Technologies" (Washington: 2020), available at https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf.

243 American Innovation and Choice Online Act of 2021, S. 2992, 117th Cong., 1st sess. (October 18, 2021), available at https://www.congress.gov/bill/117th-congress/senate-bill/2992/text.

244 Daron Acemoglu and Pascual Restrepo, "Unpacking Skill Bias: Automation and New Tasks"; Gravelle, "Wage Inequality and the Stagnation of Earnings of Low-Wage Workers."

245 Committee on Digital Platforms, "Final Report."

246 Ibid.

247 Conner, Simpson, and Halpin, "Voters Support Enacting Stronger Consumer Protections Online, Antitrust Action for Big Tech Companies."

248 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (Brussels: 2020), available at https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf, section 4, articles 26 and 27, pp. 59–61.

249 Jarsulic and others, "Reviving Antitrust."

250 Jarsulic, Gurwitz, and Schwartz, "Toward a Robust Competition Policy."

251 Committee on Digital Platforms, "Final Report."

252 American Innovation and Choice Online Act of 2021, S. 2992.

253 Khan, "Sources of Tech Platform Power."

254 Ibid.

255 Committee on Digital Platforms, "Final Report."

256 Nadler and others, "Investigation of Competition in Digital Markets."

257 Digital Competition Expert Panel, "Unlocking digital competition."

258 Competition and Markets Authority, "Online platforms and digital advertising."

259 Australian Competition and Consumer Commission, "Digital Platform Inquiry: Final Report" (Canberra, AU: 2019), available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

260 Autorité de la concurrence, "Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques," February 19, 2020, available at https://www.autoritedelaconcurrence.fr/en/press-release/autorite-publishes-its-contribution-debate-competition-policy-and-challenges-raised.

261 Bundesministeriums für Wirtschaft, "Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0," available at https://www.bmwi.de/Redaktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.pdf?__blob=publicationFile&v=10 (last accessed September 2021).

262 Jacques Crémer, Yves-Alexandre de Montjoye, and Heike Schweitzer, "Competition policy for the digital era" (Brussels: European Commission Directorate-General for Competition, 2019), available at https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

263 European Commission, "The Digital Markets Act: ensuring fair and open digital markets," December 15, 2020, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

264 Japanese Ministry of Economy, Trade and Industry, "Bill on Improving Transparency and Fairness of Specific Digital Platforms," available at https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g20109023.htm (last accessed September 2021).

265 Wheeler, Verveer, and Kimmelman, "New Digital Realities; New Oversight Solutions."

266 Tom Wheeler, "A focused federal agency is necessary to oversee Big Tech," Brookings Institution, February 10, 2021, available at https://www.brookings.edu/research/a-focused-federal-agency-is-necessary-to-oversee-big-tech/.

267 Feld, *The Case for the Digital Platforms Act: Breakups, Starfish Problems, & Tech Regulation*.

268 Scott Morton, "Reforming U.S. Antitrust Enforcement and Competition Policy."

269 European Commission, "The Digital Markets Act"; European Commission, "The Digital Services Act: ensuring a safe and accountable online environment," December 15, 2020, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

270 For more on the EU calibration of quantitative thresholds for gatekeeper designation, see European Commission, "Impact Assessment Report Accompanying the document Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act): Part 1" (Brussels: 2020), available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act, paragraphs 133 to 151, pg. 46–49.

271 A primary business unit—such as an e-commerce marketplace, social media service, search engine, or digital advertising exchange—is defined in contrast to an ancillary business unit. Examples of ancillary business units might include an automaker's in-car navigation software setup for mobile devices or a health insurance provider's eligibility look-up tool. While these services would still be subject to any applicable general online services rules, they would not alone be sufficient to also qualify businesses as gatekeeper services. Such a definition will need to be further defined to prevent abuse.

272 James Tobin and William C. Brainard, "Asset Markets and the Cost of Capital," *Cowles Foundation for Research in Economics* 427 (1976), available at https://cowles.yale.edu/publications/cfdp/cfdp-427.

273 Jarsulic, Gurwitz, and Schwartz, "Toward a Robust Competition Policy."

274 Ryan H. Peters and Lucian A. Taylor, "Intangible Capital and the Investment-q Relation," *Journal of Financial Economics* (2016), available at https://doi.org/10.2139/ssrn.2405231.

275 For more on Q ratios as indicators of monopoly rents, see Eric B. Lindenberg and Stephen A. Ross, "Tobin's Q Ratio and Industrial Organization," *The Journal of Business* 54 (1) (1981): 1–32; Jarsulic, Gurwitz, and Schwartz, "The Q ratio: Using stock market valuations to determine when firms are earning monopoly profits" in "Toward a Robust Competition Policy."

276 U.S. Department of Justice, "Competition And Monopoly: Single-Firm Conduct Under Section 2 of the Sherman Act: Chapter 2," available at https://www.justice.gov/atr/competition-and-monopoly-single-firm-conduct-under-section-2-sherman-act-chapter-2 (last accessed September 2021).

277 Khan, "The Separation of Platforms and Commerce."

278 Ibid.

279 Ending Platform Monopolies Act, H.R. 3825.

280 Ibid.

281 Augmenting Compatibility and Competition by Enabling Service Switching Act, H.R. 3849.

282 Steve Stecklow, Aditya Kalra, and Jeffrey Dastin, "Five U.S. lawmakers accuse Amazon of possibly lying to Congress following Reuters report," Reuters, October 18, 2021, available at https://www.reuters.com/technology/five-us-lawmakers-accuse-amazon-possibly-lying-congress-following-reuters-report-2021-10-18/; Geoffrey A. Fowler, "The 5 biggest little lies tech CEOs told Congress — and us," *The Washington Post,* July 29, 2020, available at https://www.washingtonpost.com/technology/2020/07/29/big-tech-ceo-hearing-lies/.

283 For example, the ABC framework from the transatlantic high-level working group on content moderation online and freedom of expression, convened by the Annenberg Public Policy Center of the University of Pennsylvania, is a good example of looking beyond content alone. Camille François proposes understanding disinformation through (A) manipulative actors and (B) deceptive behavior, alongside (C) harmful content.

284 Evelyn Douek, "The Rise of Content Cartels" (New York: Knight First Amendment Institute at Columbia University, 2020), available at https://knightcolumbia.org/content/the-rise-of-content-cartels; Keller, "Who Do You Sue?"

285 Daphne Keller, "Privacy, Middleware, and Interoperability: Can Technical Solutions, Including Blockchain, Help Us Avoid Hard Tradeoffs?", Center for Internet and Society, August 23, 2021, available at https://cyberlaw.stanford.edu/blog/2021/08/privacy-middleware-and-interoperability-can-technical-solutions-including-blockchain-0; Daphne Keller, "Some Humility About Transparency," Center for Internet and Society, March 19, 2021, available at https://cyberlaw.stanford.edu/blog/2021/03/some-humility-about-transparency.

286 For a discussion of administrability challenges in the context of network industries, see Khan, "The Separation of Platforms and Commerce"; Howard Shelanski and J. Gregory Sidak, "Antitrust Divestiture in Network Industries," *University of Chicago Law Review* 68 (2001), available at https://chicagounbound.uchicago.edu/uclrev/vol68/iss1/1/. For a discussion of the particular challenges faced by the FCC and FTC over recent years, see Chopra, "Statement of Commissioner Rohit Chopra Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security"; Tom Wheeler, "Facebook Says It Supports Internet Regulation. Here's an Ambitious Proposal That Might Actually Make a Difference," *Time*, April 5, 2021, available at https://time.com/5952630/facebook-regulation-agency/. See also Cecilia Kang, "Here's How the Telecom Industry Plans to Defang Their Regulators."

287 Din, "House E&C seeks major boost to FTC privacy efforts"; American Choice and Innovation Online Act, H.R. 3816; Lawyers' Committee for Civil Rights Under Law, "Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce," Press release, August 4, 2021, available at https://www.lawyerscommittee.org/federal-trade-commission-must-protect-civil-rights-privacy-in-online-commerce/; Sen. Richard Blumenthal and others, "Letter to the FTC encouraging a rule-making on protection consumer privacy, promoting civil rights, and setting clear safeguards on the collection and use of personal data in the digital economy," September 20, 2021, available at https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.

288 Consumer Reports and others, "Letter to House and Senate Leadership from civil rights, civil liberties, and consumer protection organizations in support of increased FTC funding in the Build Back Better Act," September 23, 2021, available at https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf; U.S. Federal Trade Commission, "FTC Appropriation and Full-Time Equivalent (FTC) History," available at https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation (last accessed April 2021).

289 Ibid.

290 Feld, *The Case for the Digital Platforms Act: Breakups, Starfish Problems, & Tech Regulation*. See chapter VIII for a thoughtful discussion of administrative options.

291 Wheeler, Verveer, and Kimmelman, "New Digital Realities; New Oversight Solutions"; Digital Competition Expert Panel, "Unlocking digital competition"; See Chapter VIII in Feld, "The Case for the Digital Platform Act," for a thoughtful discussion of administrative options; U.K. Competition and Markets Authority, "New watchdog to boost online competition launches," Press release, April 7, 2021, available at https://www.gov.uk/government/news/new-watchdog-to-boost-online-competition-launches--3.

292 Wheeler, Verveer, and Kimmelman, "New Digital Realities; New Oversight Solutions."

293 Data Protection Act, S. 2134.

294 Online Privacy Act, H.R. 4978.

americanprogress.org

1333 H Street, NW, 10th Floor, Washington, DC 20005 • Tel: 202-682-1611 • Fax: 202-682-1867