In many areas of the world, including the European Union, United Kingdom, South Korea, and Australia, governments are considering new legislation to check the market power of a few dominant technology platforms. Yet some of the most sweeping proposals are taking place within the U.S. Congress. In October 2020, the majority staff of the House Subcommittee on Antitrust, Commercial, and Administrative Law published a set of recommendations to promote competition in technology markets, the result of a 16-month investigation that directed attention to the actions of Alphabet (the parent company of Google), Amazon, Apple, and Facebook (now Meta). The House Judiciary Committee advanced six bills in June 2021 that paralleled many of these recommendations, focusing on the anticompetitive impacts of self-preferencing, mergers and acquisitions, data accumulation, and network effects related to digital platforms. Meanwhile, the Senate Judiciary Committee voted to advance the American Innovation and Choice Online Act and Open App Markets Act in early 2022.

While antitrust reform has seen broad bipartisan support in Congress, members of both parties have also expressed concerns that these bills might have unintended consequences. For example, many of the newly proposed restrictions would only apply to “covered platforms” that meet certain size or categorical criteria—which, under current market conditions, would primarily include Alphabet, Amazon, Apple, and Meta. In turn, some critics have asserted that unequal rules could create arbitrary winners or losers in the marketplace and even benefit foreign competitors or bad actors at the expense of U.S. technological innovation. To put these issues into context, below is an overview of seven major bills under consideration in the U.S. House and Senate as well as the related challenges, commentary, and controversies that surround them.
1. **American Innovation and Choice Online Act (S.2992) / American Choice and Innovation Online Act (H.R.3816)**

**ARGUMENTS FOR**

The American Innovation and Choice Online Act addresses self-preferencing, a core concern raised by the House Antitrust Subcommittee investigation. Dominant digital platforms such as Amazon.com, Apple's App Store, and Google Search wield extensive control over which products and services their hundreds of millions of users view—including their own. For example, the subcommittee investigation highlighted how Amazon's voice assistant, Alexa, had directed shopping queries to Amazon.com and had been more likely to recommend AmazonBasics products over those of third-party competitors, as well as how Alphabet had ranked its own services—such as Google Flights, Google Maps, Google Shopping (formerly Froogle), and YouTube—above competing third-party websites in Google Search results.

Self-preferencing raises challenges of both fairness and competition; it could both give dominant digital platforms a distinct advantage over their direct competitors' products or services and also prevent consumers from discovering newer, lesser-known, or potentially more innovative options. For this reason, the bill would designate certain conduct by covered platforms as “unlawful” or “discriminatory,” including those which would generally (a) give their products or services an advantage over those of other third-party businesses that use the platform or (b) otherwise discriminate among “similarly situated business users.” The House bill would prohibit these behaviors outright, while the Senate version would do so only when presented with “a preponderance of the evidence” that the actions would “materially harm competition on the covered platform.”

*Dominant digital platforms such as Amazon.com, Apple’s App Store, and Google Search wield extensive control over which products and services their hundreds of millions of users view—including their own.*

The bill also addresses other ways in which dominant platforms could potentially take advantage of their intermediary position between sellers, buyers, and advertisers. For example, Amazon has exclusive access to browsing and sales analytics that other third-party sellers do not, which it has reportedly used to introduce or improve its own product lines over those of its competitors. To overhaul this information gap, the bill contains provisions that would (a) prevent covered platforms from using any non-public data that is associated with their competitors to benefit their own goods and (b) grant third-party competitors access to the data that they generate on the platform. The overarching goal is to help small businesses and start-ups compete with established digital companies, especially in scenarios where the larger entity both controls the platform and competes on it.

**ARGUMENTS AGAINST**

Several members of Congress, including Senators Dianne Feinstein (D-CA) and Alex Padilla (D-CA), have voiced concerns that the bill could have negative ramifications on user privacy and security. It could stop covered platforms from installing or maintaining default security measures on their services, such as Google Chrome’s spam filters and malware protection. It could also prevent companies from imposing privacy or security rules for third-party businesses that use their platforms, such as Apple’s pop-up notifications that allow users to decline to be tracked across apps and websites. In addition, the bill could
**Require** algorithms such as Google Search to equally rank apps, websites, or links that may pose security risks. Moreover, the third-party data access and portability provisions could—in the absence of further privacy protections—lead covered platforms to transfer sensitive customer information to bad actors.

Both the Senate and House versions contain an exception that would allow covered platforms to present evidence that any prohibited conduct is “narrowly tailored,” “nonpretextual,” and “necessary” to either (a) comply with law, which could include a future comprehensive federal privacy law; (b) protect privacy and security; or (c) support the platform’s necessary functionality. Yet some argue that this standard is not sufficient to protect user safety because it treats privacy and security as secondary values to competition instead of as a default priority. And although the Senate version clarifies that covered platforms would not be required to hand over data to the Chinese government or other foreign state adversaries, it might not prevent the transfer of data to bad actors either within the United States or those unaffiliated with a government entity.

In addition, opponents have expressed concerns that the nondiscrimination provisions would prevent attempts by covered platforms to remove misinformation, hate speech, and other harmful content. TechFreedom, Free Press, and Representative Zoe Lofgren (D-CA) are among those who have stated that such a provision could require app stores to host extremist services such as Parler or Infowars if an antitrust enforcer viewed them as “similarly situated” to other businesses. While the Senate version attempts to address such concerns by specifying that differential treatment would only be prohibited if companies unevenly apply their terms of service in a way that could “materially harm competition,” content moderation remains a highly politicized issue that will not be easily resolved—especially as some prominent Republicans call for antitrust enforcement to prevent the alleged censorship of right-wing voices.

2. **Ending Platform Monopolies Act (H.R.3825)**

**ARGUMENTS FOR**

Like the American Innovation and Choice Online Act, the Ending Platform Monopolies Act attempts to address any unfair competitive advantages that may arise when the same company both controls access to a marketplace and simultaneously competes in it. Yet H.R.3825 proposes going further than S.2992 and H.R.3816 to holistically ban dominant platforms from offering their own products or services at all in a marketplace that it controls. It also proposes banning covered platforms from owning a line of business that otherwise presents a “conflict of interest” or that would enable the covered platform to advantage its own products or services over those of its competitors.

Proponents of this bill argue that a ban on self-preferencing does not go far enough and that it is necessary to completely separate out the vertical ownership of multiple business lines to prevent any additional abuses of market position that could occur. Since dominant platforms control algorithms and data collection in their marketplaces, often in a nontransparent manner, the bill acknowledges that an inherent power asymmetry exists between a dominant platform and third-party business users regardless of whether self-preferencing practices are banned.

**ARGUMENTS AGAINST**

H.R.3825 has seen considerable division among both parties; it narrowly passed the House Judiciary Committee with a 21–20 vote and has not yet been introduced in the Senate. Opponents argue that the bill assumes that platforms face a conflict of interest in owning multiple lines of business, even if there is no immediately obvious harm to either consumers or small businesses.
H.R.3825 would force platforms such as Amazon.com to change their business models to either discontinue brands such as AmazonBasics or structurally separate any services that the bill defines as a conflict of interest. As such, the bill could affect many popular free or low-cost services and their related platforms, including Apple’s Siri, Facebook Messenger, Google’s YouTube, and Google Maps, that may offer some convenience or benefit to consumers. Companies such as Amazon and Alphabet have argued that any fundamental changes to their business models could, in turn, hurt small businesses, which, for example, benefit from access to Amazon.com’s large e-commerce customer base and from increased visibility due to the integration of Google Search, Maps, and other services.

3. Platform Competition and Opportunity Act (H.R.3826/S.3197)

ARGUMENTS FOR
Mergers and acquisitions (M&A) have become increasingly frequent in the United States over the past four decades—a trend that has generally occurred in parallel with higher market consolidation, especially within industries most impacted by network effects and economies of scale. In the short term, M&A can enable dominant platforms to gain access to data, intellectual property, or workforce talent—and effectively eliminate current or potential competitors. The long-term effects may serve to entrench the market power of dominant platforms while simultaneously reducing consumer choice, quality of products or services, and future innovation across the industry.

The Platform Competition and Opportunity Act aims to prevent these short- and long-term anticompetitive effects through a general ban on dominant platforms acquiring current or potential competitors. It directs these concerns toward Alphabet, Amazon, Apple, and Meta, which have completed hundreds of M&A transactions over the past two decades. The House Antitrust Subcommittee investigation highlighted many examples: Google purchased Android, YouTube, DoubleClick, and AdMob; Amazon acquired Audible, Zappos, Diapers.com, and Whole Foods; Apple bought Beats Electronics, Shazam, Texture, and HopStop.com; and Facebook procured Instagram, Onavo, and WhatsApp. Proponents of the bill argue that these acquisitions ultimately helped the four companies develop and maintain control over numerous markets—including for search engines, mobile operating systems, app stores, social media, voice assistants, e-commerce, and cloud computing—at the expense of consumers and small businesses.

In the short term, M&A can enable dominant platforms to gain access to data, intellectual property, or workforce talent . . . The long-term effects may serve to entrench the market power of dominant platforms while simultaneously reducing consumer choice, quality of products or services, and future innovation across the industry.

In addition, the legislation would place the burden of proof on dominant platforms, instead of government enforcers, to prove that a proposed acquisition would not present anticompetitive harm. Under the bill, covered platforms would need to present “clear and convincing evidence” that a proposed acquisition either (a) falls under an exemption to prohibited acquisitions in section 7A(c) of the Clayton Act; (b) does not involve a current, “nascent,” or “potential” competitor that offers the same products or services; or (c) would not “enhance or increase” their market position. It also clarifies that certain non-monetary characteristics may pertain to digital platforms, such as how businesses might compete for “user attention” rather than for traditional sales, and how the
acquisition of data alone can “enhance” or “increase” a platform’s market position. While government enforcers would still face a high burden of proof to prove anticompetitive harm in any other merger challenges that do not involve covered platforms, supporters of H.R.3826 and S.3197 contend that a stronger standard is necessary to prevent anticompetitive acquisitions by the digital platforms that have the greatest potential to create harmful effects.

ARGUMENTS AGAINST
The bill would substantially alter M&A review standards for a small number of dominant companies, raising concerns that the requirement to present “clear and convincing” evidence of the absence of potential harm could create a chilling effect that would significantly decrease acquisitions by covered platforms.

Unlike H.R.3826, the Senate version partially addresses these concerns by exempting transactions valued under $50 million from the enhanced standards. Yet industry groups such as NetChoice have argued that the overall provisions could still hurt U.S. start-ups by motivating investors to operate in other countries. The possibility of future acquisition may encourage at least some start-up formation since it provides a viable exit strategy for a new company that ultimately does not become profitable. In late 2019, the Silicon Valley Bank surveyed over 1,000 technology and healthcare start-ups from four countries, finding that 58 percent of U.S. respondents cited acquisition as their “realistic long-term goal,” while just 17 percent favored making an initial public offering (IPO), and 14 percent expected to continue private ownership. As such, a reduction in acquisitions by Big Tech companies could also decrease the financial incentive for both venture-capital investors and entrepreneurs to launch new businesses—which, in turn, could potentially contradict the goals of innovation and competition that the bill aims to further.

4. Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act (H.R.3849)

ARGUMENTS FOR
In many digital markets, large companies benefit from network effects, wherein a platform becomes more powerful as the number of individuals who use it rises. For example, a person is more likely to join a social media platform that already has hundreds of millions of users—such as Instagram or Facebook—than a newer start-up that their friends and acquaintances do not spend time on. Similarly, massive customer bases provide an incentive for software developers to use and design services for Amazon Web Services, Apple’s iOS, or Google Chrome—which, in turn, helps entrench or even further grow these platforms’ number of users. Proponents of the ACCESS Act argue that intervention is necessary because each of these respective markets has reached a “tipping point” where network effects are so strong that users, advertisers, sellers, and developers have few choices other than to use a dominant platform, creating an almost insurmountable barrier to entry for potential competitors.

The ACCESS Act attempts to dismantle this barrier through two mechanisms: platform interoperability and data portability. First, it would require covered platforms to permit interoperability or cross-functionality with their competitors in compliance with standards that the Federal Trade Commission (FTC) would issue. Second, it would require covered platforms to securely transfer user-generated data to the associated individual(s) or to another business user upon request. In this regard, the bill addresses the anticompetitive effects of incumbency; a person might be discouraged from switching to a new social media start-up if all their photos, posts, and followers are currently on Instagram—unless they are either able to transfer their content or if the two platforms could engage with each other through an application programming interface (API). Some commentators have drawn parallels to the telephone industry—
which the 1996 Telecommunications Act and Federal Communications Commission rules require landline and wireless carriers to allow customers to keep their phone numbers if they switch providers—as an example of how similar regulation has lowered switching costs and benefited both competition and consumers in the past.

The ACCESS Act includes provisions to protect user privacy and security, including requiring covered platforms to take “reasonable steps to avoid introducing security risks to user data.” Supporters of the legislation argue that privacy and data portability are not incompatible values; in fact, the European Union’s General Data Protection Regulation (GDPR) grants individuals a comparable right to either download their personal data held by businesses or request to transfer it to another company, and the two leading consumer-privacy bills in the current Congress, the SAFE DATA Act and Consumer Online Privacy Rights Act (COPRA), include similar data-portability provisions. Proponents argue that data portability gives individuals more control over data related to them, including the option to transfer that data to a competing service that is potentially more privacy-protective. Finally, the bill would allow the FTC to exercise its decades-long expertise in privacy and consumer protection since it would direct the agency to establish a technical committee to create portability and interoperability standards, including any related data-protection requirements, for covered platforms.

ARGUMENTS AGAINST

Although many legislators on both sides of the aisle have supported data portability and interoperability in principle, the general lack of specific technical provisions within the ACCESS Act has created a fair amount of uncertainty. Critics argue that it would be difficult or even impossible to implement interoperability and portability in a meaningful way because the nature of data and systems is complex and decentralized. Unlike phone numbers, which are relatively uniform, platforms host data in many non-standardized formats, such as photos, communications between multiple people, and algorithmic inferences. The FTC would therefore face a significant technical challenge in developing standards to integrate data from multiple platforms and deciding which data is appropriate to export, especially data that involves multiple users.

In addition, any bill that increases third-party information sharing will also require strong privacy and security protections to prevent data breaches or interoperability with bad actors. Data portability is a provision of many current privacy laws or bills, including the GDPR, COPRA, and the SAFE DATA Act—yet, unlike the ACCESS Act, these all come with additional boundaries on how businesses may collect, use, process, and further share personal information. Without a baseline of privacy protections, data portability and interoperability alone could potentially introduce opportunities for bad actors to misuse large data sets or harm the customer bases that depend on affected platforms. For example, Facebook launched a platform in 2007 to allow developers to build and integrate apps within its social network, which, controversially, Cambridge Analytica eventually took advantage of to target political advertisements. Opponents argue that the broad statutory language within H.R.3849 could delegate too much authority to the FTC to establish data-protection standards, including what “reasonable” security measures might entail—potentially leaving regulations uncertain or inconsistent, depending on the current FTC leadership.
Without a baseline of privacy protections, data portability and interoperability alone could potentially introduce opportunities for bad actors to misuse large data sets or harm the customer bases that depend on affected platforms.

5. Merger Filing Fee Modernization Act (H.R.3843/S.228)

ARGUMENTS FOR
Over the past decade, funding and staffing levels for the FTC’s Bureau of Competition and the Department of Justice’s (DOJ) Antitrust Division have not kept pace with rising U.S. GDP and M&A activity. Although U.S. GDP increased approximately 37 percent from 2010 to 2018 and premerger filing activity under the Hart-Scott-Rodino (HSR) Antitrust Improvements Act doubled during this period, appropriations for the DOJ’s Antitrust Division and the FTC only grew around 3 percent in nominal dollars—equivalent to an 18 percent decrease after adjusting for inflation. Tighter budgets result in lower staffing levels: Brookings visiting fellow Bill Baer has testified that the DOJ’s Antitrust Division contained just 594 employees at the close of fiscal year (FY) 2019, compared to 795 employees one decade prior. In particular, the FTC and DOJ could benefit from additional resources to investigate large transactions; not only have HSR premerger notification filing fees remained the same in nominal dollars since 2001, but the largest M&A transactions (over $5 billion) generate over 18 percent of second requests while only bringing in 5 percent of premerger filing fees.

Without sufficient funding and personnel, these agencies may confront difficult decisions over which investigations or enforcement actions to prioritize. The Merger Filing Fee Modernization Act aims to address this gap through two primary channels: adjusting HSR premerger filing fee thresholds and raising congressional appropriations. First, the bill proposes increasing premerger notification filing fees for mergers valued over $500 million—including a substantial hike from $280,000 to $2,250,000 for transactions valued over $5 billion, adjusted annually for inflation. Second, it proposes an appropriations increase from $184.5 million in FY 2021 to $252 million in FY 2022 for the DOJ’s Antitrust Division, as well as from $331 million in FY 2021 to $418 million in FY 2022 for the FTC. Taken together, these provisions would improve the capacity of federal enforcement agencies to investigate and litigate any anticompetitive behavior without a substantial change in antitrust law.

ARGUMENTS AGAINST
The Merger Filing Fee Modernization Act is largely uncontroversial; within the past two years, members from both parties have publicly supported allocating additional resources to the FTC and the DOJ’s Antitrust Division. Both the House and Senate included the Merger Filing Fee Modernization Act in their separate versions of a bill to support domestic semiconductor manufacturing and supply chains: the America COMPETES Act and the United States Innovation and Competition Act. House Antitrust Subcommittee Ranking Member Ken Buck (R-CO) also wrote in his October 2020 report, The Third Way: Antitrust Enforcement in Big Tech, “We agree [with the majority side] that antitrust enforcement agencies need additional resources and tools to provide proper oversight.”
6. State Antitrust Enforcement Venue Act (H.R.3460/S.1787)

ARGUMENTS FOR
State attorneys general play a valuable role in strengthening antitrust enforcement; they can both bring additional resources to supplement federal actions as well as prioritize consumer-protection issues that affect local residents. States may file complaints under either federal or state competition law—but are subject to Judicial Panel on Multidistrict Litigation (JPML) proceedings, which permit defendants to request consolidating similar antitrust lawsuits filed by states or private plaintiffs across multiple jurisdictions. Yet many state attorneys general have argued that the involuntary centralization of state actions could both violate their sovereignty and potentially benefit defendants. When Google requested transferring State of Texas, et al. v. Google from the Eastern District of Texas to the Northern District of California in January 2021, Texas responded: “In its attempt to move this case to its own backyard, Google ignores Texas’s interest in having the rights of its citizens adjudicated in Texas. A sovereign State’s choice of forum within the State inherently carries with it the interests of its own citizenry.”

In September 2021, 30 state attorneys general wrote to House and Senate leaders to request “a [statutory] provision confirming that the states are sovereigns that stand on equal footing with federal enforcers under federal antitrust law, including with regard to the timing of challenging anticompetitive mergers and other practices.” The State Antitrust Enforcement Venue Act is one such measure that would prevent the JPML from transferring federal civil antitrust enforcement actions filed by state attorneys general to other courts or jurisdictions, thus granting states more control over the location of their proceedings and preventing any administrative delays associated with transfers.

ARGUMENTS AGAINST
The State Antitrust Enforcement Venue Act has amassed broad bipartisan support in Congress; over 100 Republicans have signed a discharge petition to call for a House floor vote, and prominent Democrats have backed it as well. Yet some critics, including those at the U.S. Chamber of Commerce and R Street Institute, argue that decentralizing such lawsuits would reduce efficiency in competition enforcement. In other words, defendants might have to answer to simultaneous proceedings across multiple districts or jurisdictions, which could subsequently drive up costs for both private companies and court systems. These critics have voiced further concern that if, hypothetically, multiple state lawsuits address similar conduct, uncertainty might arise from contrasting judicial decisions across various courts and jurisdictions.

7. Open App Markets Act (H.R.5017/S.2710)

ARGUMENTS FOR
The Open App Markets Act responds to opposition from app developers such as Epic Games, Match, Spotify, and Tile over a 15 to 30 percent commission that both Apple and Google take for all app-store sales and in-app payments. Until recently, Apple prevented iOS app developers from informing their customers of any alternative payment methods or lower prices outside of the App Store (but has recently made limited changes to permit iOS developers to email customers about external payment methods or otherwise avoid paying the commission in select contexts). To address concerns that payment restrictions hurt small businesses, entrepreneurs, and customers, the bill would prohibit covered app stores with over 50 million U.S. users from (a) limiting developers to the use of in-app payment systems; (b) requiring either equal or better pricing on their app-store and in-app payments or punishing developers for offering different pricing; and (c) preventing developers from communicating pricing offers with their customers.
More broadly, the bill aims to reduce the duopoly that Apple and Google hold over app distribution on mobile devices. These companies either prohibit or discourage users from downloading apps outside the App Store and Google Play (also known as “sideloading”) on iOS and Android devices, respectively, reinforcing their exclusive authority to develop rules that millions of developers must follow for iOS and Android users to download their apps. The ACCESS Act aims to change this paradigm by requiring covered operating systems to allow users to install third-party apps outside the dominant app store—or even to install third-party app stores on their devices. Like the American Innovation and Choice Online Act, the Open App Markets Act would prevent covered app stores from “unreasonably” self-preferencing their own apps over their competitors’ and using non-public data generated by third-party apps for their own market research—thus acknowledging Apple and Google’s competitive advantage from both controlling an app marketplace and developing apps that compete on it.

ARGUMENTS AGAINST

Opponents of the Open App Markets Act point to safety issues; both Apple and Google have stated that their developer guidelines (and associated fees) are necessary to maintain the privacy and security of the apps that users download. For example, Apple requires iOS app developers to display “privacy nutrition labels,” pass a malware screening, and obtain consent to track users across websites and apps for advertising purposes—all features that this bill could potentially block. In contrast, some of the proposed legislative provisions, especially those that would require dominant app stores to allow sideloading and give third-party developers “access to operating system interfaces, development information, and hardware and software features,” could increase risks of malware or ransomware. According to Apple, approximately 84 million malware attacks were discovered worldwide in 2019—but iOS devices (which completely ban sideloading) fell victim to an estimated 15 to 47 times fewer attacks than Android devices (which allow sideloading but warn users against it).

The bill addresses these safety concerns, in part, by allowing covered companies to take actions that (a) are “necessary to achieve user privacy, security, or digital safety”; (b) “prevent spam or fraud”; and (c) comply with law, which could include a future comprehensive federal privacy law. Yet, in the event of any tension between data protection and competition, a covered company bears the burden of proof to show that its actions are “demonstrably consistent,” “not used as a pretext to exclude,” “narrowly tailored,” and lack any other “less discriminatory and technically possible” alternatives to protect safety or security. For these reasons, opponents charge that covered app stores may face legal gray areas or uncertainty that could prevent or discourage them from taking actions to enhance security on their platforms.

Caitlin Chin is a fellow with the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2022 by the Center for Strategic and International Studies. All rights reserved.