U.S. Antitrust Legislative Proposals: A Global Perspective

U.S. Chamber of Commerce

February 2022

TABLE OF CONTENTS

I. Executive Summary

The world's leading powers are racing to develop and deploy emerging technologies, such as artificial intelligence and quantum computing, that could shape everything from the economic and military balance among states to the future of work, wealth, and inequality within them. . . . Rapid changes in technology will shape every aspect of our lives and our national interests, but the direction and consequences of the technological revolution remain unsettled. . . . America must reinvest in retaining our scientific and technological edge and once again lead, working alongside our partners to establish the new rules and practices that will allow us to seize the opportunities that advances in technology present.

- The White House, Interim National Security Guidance (Mar. 3, 2021)

The United States is locked in a race with China and Europe to scale certain foundational technologies, such as semiconductors, and to develop and deploy emerging technologies, such as artificial intelligence and quantum computing. This race has both economic and national security dimensions, given the technologies' potential military applications, as well as their impact on economic competitiveness more broadly.

Faced with this challenge, China and the European Union (EU) are pursuing aggressive and broad industrial policies to alter the competitive landscape and advance their interests to achieve world-leading status in various technologies. President Xi Jinping has stated explicitly that global tech dominance is essential to the Great Rejuvenation of the Chinese Nation, and what he hopes will be China's reassumption of global and geopolitical preeminence.[1] Similarly, in Europe leading voices including French President Emmanuel Macron have doubled down in their push for "technological sovereignty," arguing that Europe needs to band together and promote European champions for key technologies, including semiconductors, electric vehicle batteries, hydrogen, and cloud computing.[2]

The resulting policy prescriptions in China and the EU involve subsidies, discriminatory regulations, and other protectionist barriers that keep U.S. competitors at bay, while promoting domestic champions. Meanwhile, in the United States, industrial policy is a much less significant factor. Instead, private companies are the

[1] *See* "A key step to realize the Chinese dream of the great rejuvenation of the Chinese nation," People.cn (July 3, 2021).
[2] *See* "Macron calls for EU to strengthen borders and forge closer defense ties," FT.com (December 9, 2021).

driving force behind the innovation and research that determine how the U.S. will fare in this global competition.

However, Congress is considering new antitrust legislation which, perversely, would weaken leading U.S. technology companies by crafting special purpose regulations under the guise of antitrust to prohibit those firms from engaging in business conduct that is widely acceptable when engaged in by rival competitors.

A series of legislative proposals – some of which already have been approved by relevant Congressional committees – would, among other things: dismantle these companies; prohibit them from engaging in significant new acquisitions or investments; require them to disclose sensitive user data and sensitive IP and trade secrets to competitors, including those that are foreign-owned and controlled; facilitate foreign influence in the United States; and compromise cybersecurity. These bills would fundamentally undermine American security interests while exempting from scrutiny Chinese and other foreign firms that do not meet arbitrary user and market capitalization thresholds specified in the legislation.

Many members of Congress have pointed out that these proposals could damage American interests, to the benefit of China. For example, at a recent markup in the Senate Judiciary Committee on S. 2992, the American Innovation and Choice Online Act, Senator Tom Cotton (R-AR) expressed "concerns with provisions in the bill that could require data sharing between American companies and bad actors under the control of the Chinese Community Party." Similarly, Sen. John Cornyn (R-TX) explicitly criticized "the potential national security consequences of this bill." He explained that the bill "will harm American businesses and reward our adversaries, most notably the People's Republic of China … It serves our own companies up on a platter and does nothing to combat the bad conduct of our adversaries." These concerns span the aisle. Sen. Patrick Leahy (D-VT) wants to "make sure we're not inadvertently harming our national security," while Sen. Dianne Feinstein (D-CA) expressed concern "that this really is going to be very dangerous legislation. It may end up giving a very competitive advantage to large global businesses that narrowly escape being regulated by the bill." Many other members echoed these comments.

The United States has never used legislation to punish success. In many industries, scale is important and has resulted in significant gains for the American economy, including small businesses. U.S. competition law promotes the interests of consumers, not competitors. It should not be used to pick winners and losers in the market or to manage competitive outcomes to benefit select competitors. Aggressive competition benefits consumers and society, for example by pushing down prices, disrupting existing business models, and introducing innovative products and services.

If enacted, the legislative proposals would drag the United States down in an unfolding global technological competition. Companies captured by the legislation would be required to compete against integrated foreign rivals with one hand tied behind their backs. Those firms that are the strongest drivers of U.S. innovation in AI, quantum computing, and other strategic technologies would be hamstrung or even broken apart, while foreign and state-backed producers of these same technologies would remain unscathed and seize the opportunity to increase market share, both in the U.S. and globally. Indeed, during the markup of S. 2992, the bill's authors introduced a manager's amendment in an attempt to address some of these concerns. For instance, the amendment would have allowed covered entities to avoid sharing data with certain companies that are subject to U.S. sanctions or otherwise identified as a national security risk, but this amendment falls far short in its aim of protecting U.S. data and know-how from all or even most of our strategic competitors.

Instead of warping antitrust law to punish a discrete group of American companies, the U.S. government should focus instead on vigorous enforcement of current law and on vocally opposing and effectively countering foreign regimes that deploy competition law and other legal and regulatory methods as industrial policy tools to unfairly target U.S. companies. The U.S. should avoid self-inflicted wounds to our competitiveness and national security that would result from turning antitrust into a weapon against dynamic and successful U.S. firms.

Unfortunately, U.S. antitrust regulators, led by new FTC Chair Lina Khan, are already grossly misinterpreting China's ongoing antitrust reforms and drawing false equivalencies to justify an approach that would be deeply damaging to U.S. competitiveness, innovation, and national security. Chair Khan recently noted during an interview with CNBC:

> "I think it has been interesting to see China take a series of actions over the last year that actually suggested that they're going to robustly enforce the antitrust laws and their anti-monopoly laws too, right? So we're not actually seeing the type of free-for-all that was predicted. And so I think it'll be interesting to see how that continues.[3]"

In response to a question about whether China concerns are inflated, Khan continued:

> "I think it is certainly true that those arguments lose some of their force given that we've seen China go in a different direction."

Khan could not be more wrong in her interpretation of China's ongoing policy changes and actions. China's recently released Opinions on Promoting the Healthy

[3] *See* "CNBC Transcript: Federal Trade Commission Chair Lina Khan Speaks Exclusively with Andrew Ross Sorkin and Kara Swisher Live from Washington, D.C. Today," CNBC.com (January 19, 2022).

and Sustainable Development of the Platform Economy ("the Opinions")[4], in fact, appear to double down on the use of antitrust and other regulatory tools to (1) reinforce a Great Wall of data protectionism, in lockstep with other laws like the National Security Law, National Intelligence Law, Cybersecurity Law, Data Security Law, and Personal Information Protection Law; (2) strengthen industrial policy to ensure China's seizes the commanding heights in emerging technologies by creating 10,000 Chinese "Little Giants" that benefit from subsidies, tax breaks, and exemptions from regulation[5], and (3) push domestic champions to expand and deepen China's digital mercantilism abroad from a domestic market insulated from competition. Proposed U.S. legislation would supplement and perfect this intensifying effort by China – as well as ongoing efforts of the EU – to weaken American firms so that their own indigenous companies have more space in the marketplace to grow and thrive.

To be clear, the U.S. Chamber of Commerce fully supports strong enforcement of *current* U.S. antitrust law, which prevents and punishes anticompetitive conduct and promotes consumer welfare through vigorous market competition. Further, the Chamber does not question the need for a thoughtful debate about appropriately tailored and targeted legislation and regulation that addresses legitimate concerns that have arisen from the digital transformation of the economy. However, the Chamber objects to the creation or modification of antitrust laws that target particular *companies* – in this case, U.S. technology firms – instead of anticompetitive *conduct*. U.S. antitrust law should not capriciously be used to regulate or single out companies in order to manage competition, rather than promote competition in the market. Equally important, U.S. legislative proposals should not undermine U.S. economic and security interests, especially when such measures would strengthen Chinese and other foreign rivals, without any apparent benefit to U.S. consumers and workers.

Congress should reject these legislative proposals and consider embarking on the following path:

- **Operate on the overarching principle of "do no harm."** Congress should avoid giving license to foreign jurisdictions that are targeting the hard-won comparative advantage of U.S. firms. Legislation that is under consideration would amplify and excuse the mounting harm being done to the competitiveness of U.S. companies, which are critical to the United States and

[4] *See* "The Opinions of the National Development and Reform Commission and Relevant Departments on Promoting the Healthy and Sustainable Development of the Platform Economy," NDRC.gov.cn (January 19, 2022). [Guojia fazhan gaige wei deng bumen guanyu tuidong pingtai jingji guifan jiankang chixu fazhan de ruogan yijian].
[5] *See* Bloomberg, "China's Vast Blueprint for Tech Supremacy Over U.S." (January 23, 2022).

its ability to compete effectively against non-market and authoritarian regimes in a 21st-century economy.

- **Market capitalization should not be a legislative or regulatory trigger for targeting companies.** Market capitalization is a measure of future confidence in the performance of a company, not just domestically, but globally. U.S. companies with large and growing market capitalizations reach their size based on their value to markets around the world. This is a projection of American competitiveness as well as an important sign of international leadership. Further, reliance on market cap as a legislative or regulatory trigger, even when indexed for inflation, will result in additional American companies being captured as market capitalizations rise and fall independent of inflation. A one-size-fits-all approach will result in unintended and harmful outcomes to the U.S. economy.

- **Adopt narrowly tailored responses to well-documented digital economy concerns through targeted regulation, not changing antitrust laws that target particular companies.** The suggested legislation lumps together companies with distinctly different business models and competitive environments to universally respond to a collection of concerns that aren't appropriately applicable to each of the companies captured. Completing work on a federal privacy law would be one example of where a targeted legislative response to a digital economy challenge should be a priority focus of Congressional efforts.

- **Address rapidly accelerating market distortions that arise from non-market policies, including excessive concentrations under State ownership and influence.** Antitrust law in the United States is rooted in economics and enforced against private sector restraints of trade. It is not applicable against government restraints that distort competition as an effort to promote national champions, restrain the growth opportunities of foreign-based competitors, and compel technology transfer. Our antitrust laws are currently ill-equipped to address such government distortions. Congress should bolster the U.S. government's toolkit in combating non-market economy practices globally.

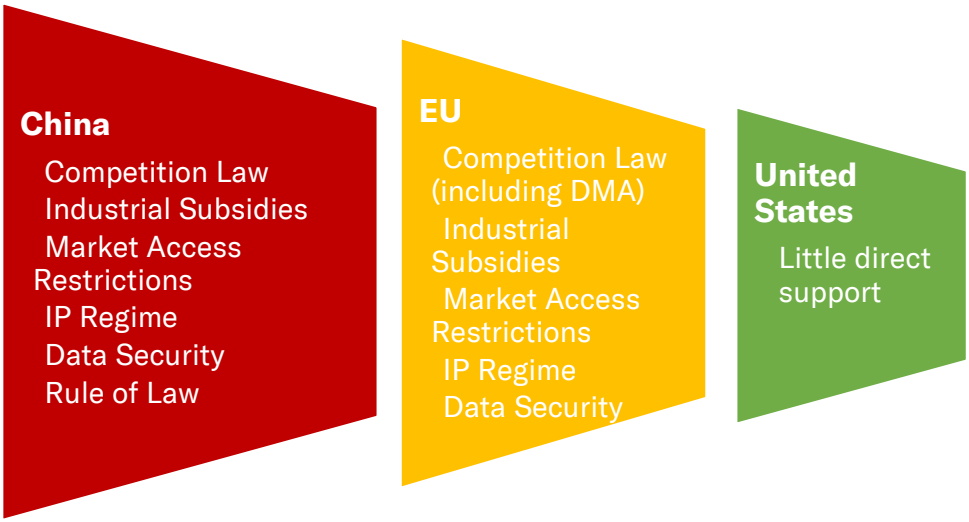
- **Institute regular briefings from the U.S. national security community to committees on how China's approach to antitrust, data, standards and technology development and acquisition policies impacts U.S. competitiveness, innovation, and national security.** These briefings should specifically include Congressional committees that do not regularly receive them (e.g., Senate and House Judiciary, Senate Finance and House Ways and Means, Senate Banking and House Financial Services, Senate and House Commerce). Such briefings for Senate and House members are critical to help

ensure that legislation is not developed in a vacuum and appropriately considers the broader context of intensifying competition with China.

If adopted, these recommendations would help the U.S. government avoid self-harm in its efforts to ensure the United States remains competitive and well-placed to maintain its national security posture.

II. Comparative Assessment of Innovation Policy in China, the EU, and the United States

Industrial Policy Support for Strategic Industries



China has mobilized its entire legal and political system in the pursuit of industrial policy goals that its leadership identifies as strategic. To a certain extent, this is true of the EU as well: with state-driven, top-down industrial policies, the EU is seeking to ensure competitiveness and "strategic autonomy" with respect to strategic technologies. Both China and the EU have introduced policies that discriminate against U.S. companies in the pursuit of these broader objectives. By contrast, the United States tends to take a more restrained policy approach to supporting particular industries, even those that are considered strategic, and has maintained a generally non-discriminatory legal and regulatory regime.

Below, we compare and contrast China and the EU on the one hand, and the United States on the other, with respect to six policy areas: competition law, industrial subsidies, market access restrictions, IP regime, data security, and rule of law. In all six areas, China actively promotes strategic industries. The EU does so in five of the six. However, at present, U.S. policy promotes strategic industries in none of the six areas, although U.S. policy is poised to become more proactive in one – industrial subsidies.

A. Competition Law

China's Anti-Monopoly Law ("AML") – the main competition law in China – is not merely a tool to promote consumer welfare and address monopolistic conduct. Rather, China also uses the AML primarily to encourage the growth and technological advancement of Chinese state-owned enterprises ("SOEs") and national champions –

both within China and, especially, overseas.[6] The U.S. Chamber of Commerce issued a detailed report on China's use of the AML as a tool of industrial policy in 2014, which enumerated concerns that have only intensified in recent years. China continues to use the AML to clear space in the marketplace for national champions and state-owned enterprises, disadvantage foreign competitors, and pressure or compel the transfer of technology to Chinese firms. China does this through all aspects of AML enforcement, including merger reviews, abuse of dominance investigations, and IP-related competition law rules. The Annex discusses China's misuse of competition law in greater detail.

As designed and until recently, the EU's antitrust regime has not been an instrument of industrial policy, nor has it been a tool to discriminate on the basis of companies' or individuals' nationality. Rather, the goal is to promote consumer welfare and ensure the proper functioning of markets. However, in recent years, EU antitrust enforcement has targeted the most prominent U.S. technology firms, in some cases on multiple occasions.[7] Indeed, European Commission President Ursula von der Leyen has said that the EU must "contain this immense power of the big digital companies" and "have mastery and ownership of key technologies in Europe."[8] In fact, EU officials' frustration with the limits of antitrust law is part of the impetus for the Digital Markets Act (DMA) – a legislative proposal that would constrain online "gatekeepers," a term defined in such a way that it includes only, or almost exclusively, large U.S. technology companies.[9] For example, EU officials complain that antitrust investigations take too long and there are "high legal thresholds to prove abuse."[10] Key negotiators of the DMA indicate that they are openly targeting a

[6] Central SOEs enjoy a limited exemption under Article 7, and combinations between SOEs are not subject to merger review because the parties are under common ownership.
[7] *See* Reuters, "Factbox: U.S. tech giants in the EU antitrust crosshairs" (Apr. 30, 2021).
[8] Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme (Nov. 27, 2019), *available at* https://ec.europa.eu/commission/presscorner/detail/en/speech_19_640. Similarly, EU Commissioner for Competition Margrethe Vestager has stated that European regulators are "vigilantly enforcing our competition rules so that we make sure that you cannot just destroy future competition, that you cannot lean on a neighboring market to your own benefit." *See*, Margarethe Vestager, interview by Kara Swisher, Sway (podcast), N.Y. TIMES (June 10, 2021).
[9] In particular, under the current draft of the DMA, a company providing a core platform service will be regulated as a gatekeeper under the DMA when the company meets the following metrics: (a) annual turnover in the European Economic Area ("EEA") at or above EUR 8 billion in the past three years or market value of at least EUR 80 billion in the last year and core platform service provision in at least three EU member states; and (b) provision of one or more core platform services, each of which has more than 45 million monthly end-users in the EEA and more than 10,000 yearly business users in the EEA in each of the last two years. DMA, Art. 3. This definition would encompass various large U.S. technology companies, and it is unclear if any EU companies would be covered.
[10] Digital Markets Act Impact Assessment support study (Dec. 2020) ("Impact Assessment support study") at 17.

handful of US companies.[11] The EU will likely decide in 2022 whether to adopt the DMA (which is discussed in greater detail in the Annex). Thus, while the EU's competition law regime itself may not be an instrument of industrial policy, at least on its face, the EU is poised to impose an industrial policy overlay through the DMA.

By contrast, the U.S. antitrust regime is not an instrument of industrial policy. Enforcement agencies do not discriminate on the basis of companies' or individuals' nationality. Rather, the goal is to promote consumer welfare and ensure the proper functioning of markets. Furthermore, U.S. antitrust enforcement agencies do not have any enforcement priorities that reflect a focus on foreign firms or the promotion of particular industries considered strategic. In addition, as in the EU,[12] the United States is considering changes to antitrust law – except these changes would disadvantage the United States' own technology companies, rather than discriminating against foreign rivals.

Thus, on balance, China uses competition law to strengthen its own domestic technology sector and enhance national competitiveness, and the EU does so as well in certain respects, and may do so much more in the future if the DMA is enacted. However, the United States does not.

B. Market Access Restrictions

China generally excludes almost all of the largest U.S. technology firms from providing their flagship products and services in China's market – effectively cutting them off from the world's second-largest economy and approximately one-sixth of the world's population. No U.S. search engines or social media companies currently operate in China, and even U.S. e-commerce companies operate in only a limited capacity, each despite their ubiquity in much of the rest of the world. The affected firms – such as Amazon, Facebook, Google, and Microsoft – are also leaders in strategic technologies such as AI, quantum computing, and cloud-related technologies. The Chinese government has also limited market access for U.S. ICT companies, for example through requirements that hardware be "secure and

[11] https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b

[12] China is also considering changes to the AML. *See* Draft Amendment to AML, *available at* http://www.google.com.hk/url?esrc=s&q=&rct=j&sa=U&url=http://www.npc.gov.cn/flcaw/flca/ff8081817ca258e9017ca5fa67290806/attachment.pdf&ved=2ahUKEwjF5NHbvJf1AhVIZcAKHX20BSMQFnoECAUQAg&usg=AOvVaw04p7xD1ZeNJR9Zd3XiBdMn.

controllable" or "secure and reliable."[13] Accordingly, China's market access restrictions significantly reduce U.S. technology companies' revenues and impair U.S. competitiveness overall.

The EU does not formally restrict U.S. technology companies' access to its market. However, the EU's emerging "digital sovereignty" agenda seeks to limit such access in practice. For example, if enacted, the DMA will impose onerous restrictions on large U.S. technology companies, including requiring U.S. companies to disclose intellectual property, sensitive trade secrets, proprietary data, and source code for algorithms. Because Chinese companies are carved out of the scope of the DMA, U.S. companies will be burdened and restricted, while Chinese companies are left free to capture the European market. The net result is an online competitive environment skewed to disfavor U.S. companies and artificially boost their EU rivals.

Future EU initiatives related to the digital sovereignty initiative, such as the forthcoming Data Act and the SecNumCloud scheme, may further limit U.S. companies' access to the EU market.[14] Moreover, the EU maintains significant nontariff barriers that affect a variety of industries, including those that are technology-intensive.[15]

By contrast, the U.S. market remains largely open to foreign technology companies, including those from China and the EU. Exceptions are narrow and based on national security concerns. Although the Trump Administration sought to prevent TikTok and other Chinese apps from accessing the U.S. market on national security grounds, the Biden Administration removed these restrictions, and currently TikTok, WeChat, and other social media apps owned by Chinese companies – as well as those owned by EU and other foreign companies – remain freely accessible within the United States.

---

[13] *See, e.g.*, Chris Burt, "China Removes Cisco, Others from List of Approved Government Service Providers," DATA CENTER KNOWLEDGE (Feb. 26, 2015); Kate Lyons, "China tells government offices to remove all foreign computer equipment," THE GUARDIAN (Dec. 8, 2019); *see also* Agatha Kratz & Janka Oertel, "Home advantage: How China's protected market threatens Europe's economic power," EUROPEAN COUNCIL ON FOREIGN RELATIONS, Policy Brief (Apr. 2021), at 4 (explaining China's use of "trade barriers or joint venture requirements to condition market access in sectors such as general aviation and telecommunications services").

[14] https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/

[15] *See generally* Office of the U.S. Trade Representative, "2021 National Trade Estimate Report on Foreign Trade Barriers" (Mar. 2021), at 177-228.

Thus, on balance, China and the EU use market access restrictions to strengthen their own domestic technology sectors and enhance national competitiveness – while the United States does not.

C. Industrial Subsidies

China grants massive subsidies to Chinese industry, particularly for economic sectors deemed strategic – such as the semiconductor sector, artificial intelligence (AI), cloud computing, synthetic biology, autonomous vehicle technology, and new energy vehicles.[16] These subsidies take the form of direct financial support (*e.g.*, grants, tax breaks, and investment), as well as preferential treatment by regulators and in the context of government and SOE procurement. The objective of such subsidies is to ensure that China and its industry are at the forefront of the economy of the future – including by displacing leading U.S. technology companies. Long-term industrial policy plans, such as Made in China 2025, describe these ambitions in detail.

The scale of China's subsidies is unrivaled worldwide. For example, the Semiconductor Industry Association estimates that since 2011, China has granted $100 billion in subsidies to its semiconductor sector.[17] In addition, U.S. Government officials have estimated that China spent $70 billion on artificial intelligence systems through 2020.[18] In 2020, China's Ministry of Industry and Information Technology announced plans to contribute about $1.4 trillion in investment over the next five years into AI, data centers, mobile communications, and other projects.[19]

Huawei is one example of Chinese industrial subsidies creating a global corporate juggernaut. A Wall Street Journal investigation identified $75 billion of tax breaks, loans, credits and other financing provided by the Chinese government to Huawei over a 20-year span from 1998 to 2019.[20] In addition, Huawei has benefited from protectionist government policies that prevent foreign companies from competing in the domestic Chinese telecommunications market, and received significant support from the Chinese government's campaign to pressure developing economies to hire Huawei to build their telecommunications networks.[21] Large credit

---

[16] 2021 Report to Congress, U.S.-China Economic and Security Review Commission (Nov. 2021), at 7-8.
[17] *See* "U.S. Needs Great Semiconductor Manufacturing Incentives," SEMICONDUCTOR INDUSTRY ASSOCIATION, *available at* https://www.semiconductors.org/wp-content/uploads/2020/07/U.S.-Needs-Greater-Semiconductor-Manufacturing-Incentives-Infographic1.pdf
[18] Ashwin Acharya & Zachary Arnold, "Chinese Public AI R&D Spending: Provisional Findings, CENTER FOR SECURITY & EMERGING TECHNOLOGY (Dec. 2019).
[19] *See* Liza Lin, "China's Trillion-Dollar Campaign Fuels a Tech Race With the U.S.," THE WALL STREET JOURNAL (June 11, 2020).
[20] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," THE WALL STREET JOURNAL (Dec. 25, 2019).
[21] Jonathan E. Hillman, "Huawei Strikes Back," FOREIGN AFFAIRS (Nov. 9, 2021).

facilities provided by the Export-Import Bank of China and China Development Bank are another key source of industrial subsidies for companies that work in key industries like telecommunications. According to a European Commission investigation, Huawei received an estimated $30 billion credit facility from Chinese state-owned banks, while its competitor ZTE enjoyed a similar $25 billion credit facility in 2009, dwarfing its revenue in 2009 of $8 billion.[22]

The EU grants subsidies based on similar industrial policy objectives, albeit on a smaller scale. Examples include Gaia-X, which would subsidize the development of European data infrastructure and cloud service providers with the goal of displacing U.S. technology companies that provide similar services, such as Amazon, Google, Microsoft, and Oracle. Gaia-X involves a total of €186.8 million committed thus far – a figure that will likely increase.[23] In addition, since the autumn of 2020, the European Commission and 11 member states have begun developing an Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services ("IPCEI-CIS"), a new funding scheme that will facilitate EU member states' direct subsidies to the cloud services sector. Germany has allocated a total of €750 million to the IPCEI-CIS.[24] With respect to quantum computing, in 2020, Germany committed €2 billion in funding by 2025,[25] and in 2021, France announced a financing plan of €1.8 billion for quantum technologies by 2025.[26] These rapidly growing subsidies to the digital sector are in addition to longstanding EU subsidies to aerospace, agriculture, and other sectors.[27]

By contrast, the United States is a relatively new entrant to the industrial subsidies arena. Historically, the United States has refrained from subsidies to promote particular industries, preferring instead to fund efforts to develop foundational technologies that can advance technology in general. However, the U.S. Congress took a new approach in 2020, passing the CHIPS for America Act to

---

[22] Matthew Dalton, "EU Finds China Gives Aid to Huawei, ZTE," THE WALL STREET JOURNAL (Feb. 3, 2011).
[23] Federal Ministry for Economic Affairs and Energy, *GAIA-X entering its operational phase* (Mar. 15, 2021).
[24] These funds have been secured thanks to the approval of the German Recovery and Resilience Plan by the EC. Federal Ministry for Economic Affairs and Energy, *Cloud IPCEI entering next phase as call for expressions of interest is launched in Germany and preparations for European matchmaking process get underway* (July 9, 2021).
[25] Federal Ministry for Economic Affairs and Energy, *Economic Affairs Ministry provides €878 million for quantum technologies* (May 11, 2021); Federal German Government, *Germany's first quantum computer in operation* (June 15, 2021).
[26] French Republic, Business France Agency, *€1.8 billion in funding for quantum technologies* (Jan. 21, 2021).
[27] *See generally* Office of the U.S. Trade Representative, "2021 National Trade Estimate Report on Foreign Trade Barriers" (Mar. 2021), at 177-228.

subsidize domestic semiconductor production.[28] As of yet, Congress has not authorized funding for the CHIPS Act.[29] Even if it does, however, U.S. subsidies for companies in strategic industries, beyond basic research, will remain limited.

Thus, China and to a lesser extent the EU use industrial subsidies to strengthen their own domestic technology sectors and enhance national competitiveness – while the currently United States does not.

D. IP Policy

For decades, China has used the misappropriation and forced-localization of IP to advance its development strategy. In a report issued in 2018 pursuant to an investigation under Section 301 of the Trade Act of 1974, the Office of the U.S. Trade Representative found that China engaged in practices to require or pressure the transfer of valuable U.S. technology and IP to China; deprived U.S. companies of the ability to set market-based terms in technology-related licensing negotiations; directed and facilitated outbound Chinese investment targeting U.S. companies and assets in key industry sectors, including to acquire their technology; and engaged in unauthorized intrusions into U.S. commercial computer networks or cyber-enabled theft of trade secrets of other proprietary information.[30] USTR found that these practices cost the U.S. economy at least $50 billion per year.

China's efforts to undermine foreign IP and pressure or compel the transfer of technology to Chinese firms takes many forms. For example, Chinese courts increasingly use antitrust principles to undermine foreign companies' IP rights. In June 2021, an intermediate court in Zhejiang Province invoked the "essential facilities" doctrine to hold that a Japanese company's refusal to license patents to Chinese companies constituted an abuse of its dominant market position.[31] The case remains in litigation. Since the case was first filed, China's State Administration for Market Regulation ("SAMR"), now the integrated competition law enforcement agency, issued Anti-Monopoly Guidelines in the Field of Intellectual Property Rights ("IP Guidelines"), which strengthen SAMR's ability to penalize foreign companies for negotiating assertively in licensing negotiations with Chinese parties, or refusing to license IP for

---

[28] *See* Public Law No. 116-283, Title XCIX – Creating Helpful Incentives to Produce Semiconductors for America, Sections 9901-9908; *see also* Ana Swanson & Don Clark, "Lawmakers Push to Invest Billions in Semiconductor Industry to Counter China" N.Y. TIMES (June 11, 2020).

[29] Daniel Flatley & Laura Litvan, "China Bill With Semiconductor Aid to Be Included in U.S. Defense Measure," BLOOMBERG NEWS (Nov. 15, 2021).

[30] *See generally* Office of the U.S. Trade Representative, "Section 301 Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation," (Mar. 27, 2018).

[31] Anjie Law Firm, "Essential or Not? The Perils of Mandatory Licensing for Non-SEPs in China: Case Comments on Four Local Rare Earth Magnet Companies v. Hitachi Metals," CHINA LAW VISION (Sept. 2, 2021).

otherwise legitimate reasons (*e.g.*, fear of misappropriation). In another worrisome trend beyond the domain of competition law, China's judiciary has recently begun to grant so-called "anti-suit injunctions" that prevent foreign IP holders from enforcing their IP rights against Chinese companies in foreign jurisdictions. Thus, it appears that China is moving towards a legal regime that curtails foreign companies' IP rights and pressures them to accept IP infringement if the infringers are Chinese.

By contrast, the EU's current IP regime is strong, and EU courts are independent. However, the EU's proposed DMA would weaken U.S. tech companies' IP rights, requiring gatekeepers (which, as noted above, is a term defined to include U.S. technology companies, while excluding most or all EU companies) to provide their EU, Chinese, Russian and other competitors access to ranking and other data generated through individual users' online search activity.[32] In essence, this would force U.S. companies to disclose valuable trade secrets to competitors from the EU and elsewhere. In addition, more generally, the DMA would undermine the value of investments that U.S. technology companies have made in developing their own proprietary digital ecosystems – for example, by mandating interoperability with third-party apps and app stores, including those developed by foreign competitors. Thus, the DMA will undermine U.S. technology companies' IP rights, and the value of their IP, to benefit EU competitors.

The U.S. legal system, on the other hand, respects and upholds IP rights for foreign and domestic companies alike. Indeed, the United States sets the global standard for protecting inventors, creators, and entrepreneurs, ranking first in the 2020 International Intellectual Property Index released by the U.S. Chamber of Commerce's Global Innovation Policy Center.[33] The United States' score was 47.64 out of 50. By contrast, China ranks 28th, with a score of 25.48 out of 50.

Thus, on balance, China uses its IP regime to undermine foreign IP and strengthen its own domestic technology sector. The EU is poised to do the same through the DMA. By contrast, the United States maintains a strong, rules-based, non-discriminatory IP regime.

E. Data Security Regime

[32] Article 6(1)(j) of the proposed DMA provides that gatekeepers must "provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data[.]"

[33] *See* Leigh Hartman, "U.S. leads world in intellectual property protection," SHARE AMERICA (May 21, 2020)

China has imposed a complex and burdensome data security regime that severely restricts cross-border transfers of information that are routine in the ordinary course of business and are fundamental to business activity. In addition, China's data security regime requires companies to hand over data to Chinese government authorities upon request. The legal regime includes China's Cybersecurity Law (effective 2017), which ushered in a series of new laws and regulations on national security reviews, data localization, and data privacy. Furthermore, in 2021 alone, China has adopted a new Data Security Law (effective September 2021) and the Personal Information Protection Law (effective November 2021), among others. This complex data security regime is part of the reason that many U.S. technology companies are unable to operate in China – and it appears to have contributed to the recent exits of Microsoft's LinkedIn and Yahoo from China.[34] The data security regime also makes it difficult for foreign companies in a range of other industries to do business in China.

The EU also imposes onerous requirements related to data privacy. For example, the EU's General Data Protection Regulation restricts the transfer of personal data outside the European Economic Area ("EEA").[35] In addition, a 2020 European Court of Justice (ECJ) decision known as *Schrems II* introduced significant uncertainty regarding the legality of the transfer of personal data outside the EEA.[36] Furthermore, following the ECJ's *Schrems II* decision, several European countries' data protection authorities invoked *Schrems II* to justify limiting U.S. technology

[34] Liza Lin, "Yahoo Pulls Out of China, Ending Tumultuous Two-Decade Relationship," THE WALL STREET JOURNAL (Nov. 2, 2021); Aaron Tilley & Liza Lin, "LinkedIn Social Network Is Leaving China, but Microsoft Remains, THE WALL STREET JOURNAL (Oct. 15, 2021). LinkedIn and Microsoft's Bing search engine along with hundreds of locally-developed apps were notified by the Cyberspace Administration of China that they had excessively collected and illegally accessed users' personal information. *See* "Announcement of the illegal collection and use of personal information by 105 apps including Douyin," Cyberspace Administration of China (May 21, 2021); *see also* Zen Soo, "China authorities name 105 apps for improper data practices," ASSOCIATED PRESS (May 21, 2021).

[35] The EEA consists of the EU member states, as well as Iceland, Liechtenstein, and Norway.

[36] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Case No. C-311/18 [2020] (Grand Ct.) (Ir.). The judgment invalidated a prior European Commission decision regarding the adequacy of the protection provided by the EU-U.S. Privacy Shield Framework. The European Court of Justice confirmed that Standard Contractual Clauses ("SCCs") are a valid personal data transfer mechanism, but stated that companies must verify, on a case-by-case basis, whether the law in the third country to which the data are transferred ensures adequate protection, under EU law. Where this is not the case, companies must either provide additional safeguards to guarantee adequate protection of the transferred data or suspend transfers. The EC adopted new, updated SCCs, taking account of the *Schrems II* judgment, on June 4, 2021.

companies' access to digital markets in Europe.[37] All of this confers a significant competitive advantage on EU technology firms, relative to U.S. and other foreign rivals.

In addition, as noted above, the DMA would require companies deemed gatekeepers – essentially, U.S. companies – to provide their EU, Chinese, and other competitors access to all "ranking" and other data generated by users of online search engines. The DMA would also prohibit gatekeepers from sharing user data across their own different services, even for the purpose of enhancing cybersecurity (*e.g.*, when data generated by one service reveals a cybersecurity threat), unless the European Commission grants an exemption.[38]

Furthermore, the EU is developing a Data Act that may result in further risks for U.S. businesses operating in Europe. While the legislative proposal in question has not yet been published, the EU Data Act may mandate further data sharing between businesses or between businesses and governments. Initial drafts also call for increased data localization for non-personal data. In addition, France is poised to take data security restrictions a step further, by effectively excluding foreign companies from the cloud services market. In particular, in October 2021, France's national data security agency published for public consultation a new version of its cloud security certification scheme (SecNumCloud), which not only include data localization requirements, but also disadvantages – and effectively precludes – foreign-owned companies from providing cloud services to government agencies and approximately 600 firms that operate "vital" and "essential" services.[39]

By contrast, the United States has no law imposing a national standard on the treatment or cross-border transfer of data. Thus, on balance, while China and the EU

---

[37] For example, the Hamburg DPA warned that the Senate Chancellery's use of the popular U.S. videoconferencing application Zoom violated the GDPR in light of the *Schrems II* decision. *See* Natasha Lomas, "Stop using Zoom, Hamburg's DPA warns state government," TECHCRUNCH (Aug. 17, 2021). In addition, France's DPA recommended that French services handling health data should avoid using American cloud services at all, even if the American company processes data entirely in the EU. *See* Romain Dillet, "France's Health Data Hub to move to European cloud infrastructure to avoid EU-US data transfers," TECHCRUNCH (Oct. 12, 2020).

[38] *See* DMA, Art. 9.

[39] *See* Nigel Cory, "'Sovereignty Requirements' in French – and Potentially EU – Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners," INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Dec. 10, 2021), *available at* https://itif.org/publications/2021/12/10/sovereignty-requirements-france-and-potentially-eu-cybersecurity. Specifically, the new regulations provide that foreign companies may not possess individually more than 25%, and collectively 39% of the value and voting rights, of a company providing the relevant cloud services; furthermore, foreign companies may not have veto rights or the ability to nominate a majority of board members for companies providing the relevant cloud services.

maintain data protection regimes that confer significant competitive advantages on domestic companies that handle personal data, the United States does not.

F. Rule of Law

For China, the law is in part a political instrument to make the state more efficient under "rule by law." However, China rejects certain aspects of Western government systems, such as an independent judiciary and separation of powers, which are essential to ensuring "rule of law". In its first "Plan on Building the Rule of Law in China (2020-2025),"[40] China refers to this as "socialist rule of law with Chinese characteristics" – a system where Marxist-Leninist legal concepts remain fundamental, and which is increasingly shaped by the so-called Xi Jinping Thought on the Rule of Law. In this system, the law is subordinated to political objectives.[41]

Advancing China's industrial policies is one of these political objectives. Although China's legal system is mature and sophisticated, it can bend in a direction that supports broader industrial policy objectives. For example, Chinese competition law regulators launched spurious investigations in 2013 and 2014 into Western companies, including Microsoft and Qualcomm.[42] More recently, certain Western business executives were detained in China during the height of the "trade war" with the United States, including an executive of Koch Industries who was reportedly interrogated about U.S. trade policies vis-à-vis China.[43] The Chinese government has been even more willing to deploy strong-arm tactics that do not reflect rule-of-law principles when foreign companies or their employees publicly voice opinions that differ from China's official stance on sensitive political issues.[44]

By contrast, both the EU and the United States operate according to a rule of law system, with an independent judiciary that applies the law impartially, without regard to political or industrial policy objectives. Thus, in this respect as well, China more strongly promotes industrial policy objectives – and in particular, the assertion of leadership with respect to strategic technologies – than the EU and the United States.

---

[40] *See* "China issues plan on building rule of law," XINHUA (Jan. 10, 2021); *see also* Plan on Building the Rule of Law in China (2020-2025) (translation available from China Law Translate).
[41] "Strengthen the Online Penetration of the People's Courts in Public Opinion," LEGAL DAILY (Dec. 8, 2021).
[42] *See* "China Harasses U.S. Tech Companies," Opinion, N.Y. TIMES (July 31, 2014).
[43] Paul Mozur, Alexandra Stevenson & Edward Wong, "Koch Executives Harassment in China Adds to Fears Among Visitors," N.Y. TIMES (July 11, 2019).
[44] *See, e.g.*, Brenda Goh & John Ruwitch, "China cracks down on foreign companies calling Taiwan, other regions countries," REUTERS (Jan. 12, 2018); Ben Cohen, "The NBA Feels a Backlash in China After a Tweet Supporting Hong Kong," THE WALL STREET JOURNAL (Oct. 7, 2019).

III. Proposed U.S. Antitrust Legislation Would Hamper the United States' Own Technological Development, While Promoting China's and the EU's Technological Advancement

Congress is considering a draft of antitrust legislation that would represent a radical departure from modern principles of antitrust law, which focuses primarily on promoting consumer welfare. The legislation at issue includes several bills in a package that the House Judiciary Committee approved in June 2021: the American Choice and Innovation Online Act ("ACIOA"); the Ending Platform Monopolies Act; the Platform Competition and Opportunity Act; and the Augmenting Compatibility and Competition by Enabling Service Switching ("ACCESS") Act.[45] In August 2021, the Open Aps Market Act was introduced in the House and the Senate.[46] In addition, in October 2021, Senators Amy Klobuchar, Chair of the Subcommittee on Competition Policy, Antitrust, and Consumer Rights, and Chuck Grassley, Ranking Member of the Judiciary Committee, introduced a bill that is similar to the ACIOA, entitled the American Innovation and Choice Online Act ("AICOA") (in January 2022, the Senate Judiciary Committee passed AICOA out of committee on a 16-6 vote, though a large majority of members expressed serious concerns about the bill's effect on national security, data security, privacy, and competitiveness).[47] And in November 2021, Senators Klobuchar and Tom Cotton introduced the Platform Competition and Opportunity Act, a companion to the House bill of the same name.[48]

The legislation would apply only to companies ("covered platform operators") that meet specific criteria based on the number of U.S. users and market capitalization – and at present, under most of the bills, only large U.S. technology companies would qualify. The legislation would dismantle such companies; prohibit them from engaging in significant new acquisitions or investments; force them to rollback or keep from offering unique products and services that benefit consumers; require them to disclose user data to competitors, including those that are foreign-owned and controlled; and facilitate foreign influence and misinformation in the United States while compromising cybersecurity. Meanwhile, with a few exceptions, foreign firms would remain unaffected. Additional details on the legislation are in the Annex.

Thus, the proposed antitrust legislation would undermine the United States in the technological competition with China, the EU, and other global powers. In

[45] American Choice and Innovation Online Act (ACIOA), H.R. 3816 § 2(g)(4), 117th Cong. (2021); Ending Platform Monopolies Act, H.R. 3825 § 5(5), 117th Cong. (2021); Platform Competition and Opportunity Act, H.R. 3826 § 3(d), 117th Cong. (2021); Augmenting Compatibility and Competition by Enabling Service Switching Act, H.R. 3849 § 5(6), 117th Cong. (2021).
[46] S. 2710, H.R. 5017, 117th Cong. (2021).
[47] S. 2992, 117th Cong. (2021).
[48] Platform Competition and Opportunity Act, S. 3197, 117th Cong. (2021).

particular, it would erode U.S. technological leadership with respect to critical technologies; expose U.S. citizens' data to misuse and misappropriation by foreign actors; and undermine the cybersecurity of U.S. technology platforms. Moreover, there would be no apparent countervailing benefit in terms of consumer welfare that offsets these steep costs.

A. Undermining U.S. Technology Leadership

China is pursuing a national quest to overtake U.S. companies in domains such as artificial intelligence, quantum computing, 5G communications technology, and a range of related industries, through the global commercial success of behemoths like Huawei, Alibaba, and Tencent. In addition, the EU has launched a series of industrial policy initiatives aimed at achieving "digital sovereignty" and "strategic autonomy" in the domain of technology, as discussed above. Meanwhile, the proposed U.S. antitrust legislation would clear away the most formidable competitors for China and the EU: U.S. technology companies.

A November 2021 study by two professors at Duke University's Fuqua School of Business details how the proposed U.S. antitrust legislation would erode U.S. competitiveness with respect to five types of technology of strategic and economic importance: quantum information science, AI, advanced communications technologies (*e.g.*, 5G), high-performance computing (*e.g.*, semiconductors), and robotics. The study finds that at present, U.S. firms generally lead in these industries, although foreign firms – particularly those from China – are challenging U.S. leadership.[49] As a result, the United States is losing its historic lead in innovation – with China quickly catching up in R&D investments and R&D intensity, and Chinese firms narrowing the gap and even taking the lead in key segments critical for global technological leadership.[50] The study finds that corporate research is vital for preventing further erosion of America's leadership, especially in digital technology; and that commercial scale and scope enable U.S. firms to invest in scientific research.[51] Indeed, companies like Google and Amazon are investing tens of billions of dollars per year in R&D in quantum computing, responsible AI, and other emerging technologies.[52] The study notes that "[c]orporate research labs can do what

[49] *See* Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 17.
[50] *See* Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 3.
[51] *See* Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 3, 43.
[52] *See, e.g.*, Sara Castellanos, "Google Aims for Commercial-Grade Quantum Computer by 2029," THE WALL STREET JOURNAL (May 18, 2021); Tom Simonite, "Amazon Joins Tech's Great Quantum Computing Race," WIRED (Dec. 2, 2019); Matt Day, Giles Turner & Yaacov Benmeleh, "Amazon is laying the groundwork for its own quantum computer," BLOOMBERG (Dec. 1, 2020).

universities and startups cannot – integrate science and technology to produce breakthrough innovations."[53] In addition, the study finds that "[t]o invest in large scale scientific research, and to create market-leading innovations, tech firms must be permitted to pursue large commercial scale and a wide range of product applications."[54] However, according to the study, the antitrust legislation would prevent such companies from developing new products or entering new markets, and will reduce their investments in research and further undermine U.S. leadership in emerging technologies.[55]

Similarly, the National Security Commission on Artificial Intelligence stated, "more and better data, fed by a larger consumer/participant base, produce better algorithms, which produce better results, which in turn produces more users, more data, and better performance."[56] Similarly, success in quantum computing requires operating at great scale and investing significant long-term resources – not just to build a fault tolerant quantum computer, but also to train a workforce to use it, and to identify applications enabled by today's quantum computers.

However, the proposed U.S. antitrust legislation would hamstring and even dismantle U.S. companies that are the leading investors in R&D. It would jeopardize their scale and scope, which currently enables them to invest and innovate in strategic technologies like AI and quantum computing. According to the study by the Fuqua professors, this would "hurt American economic prosperity and security."[57]

In a recent letter to Congress, 12 former U.S. national security officials expressed significant concerns about the legislative proposals, stating: "Recent congressional antitrust proposals that target specific American technology firms would degrade critical R&D priorities, allow foreign competitors to displace leaders in the U.S. tech sector at home and abroad, and potentially put sensitive U.S. data and IP in the hands of Beijing."[58] Similarly, in a recent op-ed, former National Security Advisor Robert O'Brien stated:

---

[53] *See* Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 55.
[54] *See* Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 62.
[55] Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 3.
[56] The National Security Commission on Artificial Intelligence, Final Report (Mar. 2021), at 26.
[57] *See* Ashish Arora & Sharon Belenzon, *American Innovation Under Threat: Restrictive Legislation and Global Competition*, Innovation Frontier Project, at 63.
[58] Letter from National Security Officials to the Hon. Nancy P. Pelosi and the Hon. Kevin O. McCarthy (Sept 15, 2021), *available at* https://s3.documentcloud.org/documents/21062393/national-security-letter-on-antitrust.pdf.

> {T}hese bills hand increased authority to bureaucrats at the Federal Trade Commission and lay the groundwork for dismantling America's most successful technology companies—the ones at the forefront of the race to retain U.S. dominance in fields such as quantum and AI. Chinese firms like Tencent, Bytedance, Alibaba, Huawei and Baidu are seeking to supplant U.S. companies and would have an open field world-wide and in America if these bills pass.[59]

Put simply, the legislation would weaken America and strengthen our rivals.

B. Risk of Misuse of U.S. Consumer Data by Foreign Actors

The proposed antitrust legislation (specifically, the ACIOA, which is being considered in the House of Representatives, and the companion bill in the Senate, the AICOA), would require large U.S. technology companies to provide user data, including data generated through business interactions with U.S. citizens, to any other company upon request, whether located in the United States or elsewhere.[60] During AICOA's markup, the bill's authors introduced a manager's amendment in an attempt to partially address some of these concerns. In addition, the ACCESS Act would require such companies to create the technical infrastructure to facilitate the transfer of such user data to other companies upon request.[61] The companies that receive the relevant data could be located in the United States or anywhere else in the world.

Thus, there is a significant risk that companies receiving ported data would turn the data over to foreign government authorities or use them for other nefarious purposes. This would not only compromise the security and privacy of U.S. citizens' data but would also facilitate foreign governments' global intelligence collection and identification of what they perceive to be external threats – potentially in direct conflict with U.S. interests and values.

In fact, the legislation implicitly recognizes the risk that these provisions pose to privacy and cybersecurity and seeks to preempt them. In particular, the ACIOA and AICOA would establish an "affirmative defense" that theoretically would allow companies to disregard the data transfer requirements in the name of privacy or cybersecurity. However, as discussed below and in the Annex, this defense is so narrow that it would likely be useless in practice. Furthermore, the ACCESS Act contains no such exception. Instead, it merely asserts that a company receiving "ported user data . . . shall reasonably secure any user data it acquires, and shall take reasonable steps to avoid introducing security risks to data or the covered platform's

---

[59] Robert O'Brien, "Breaking Up Tech Is a Gift to China," THE WALL STREET JOURNAL (Dec. 26, 2021).
[60] *See* American Choice and Innovation Online Act (ACIOA), H.R. 3816 § 2(b)(4), 117th Cong. (2021); American Innovation and Choice Online Act (AICOA), S. 2992 § 2(b)(4), 117th Cong. (2021).
[61] *See* Augmenting Compatibility and Competition by Enabling Service Switching Act, H.R. 3849 § 3(a), 117th Cong. (2021)

information systems."[62] However, laws in China, Russia, and other jurisdictions can require companies to turn over data to government authorities upon request, and without a warrant. Furthermore, the governments of China and Russia themselves, or through their proxies, have exhibited a pattern of engaging in malicious cyberattacks and intelligence gathering operations, including against U.S. citizens and the U.S. Government itself. Thus, a provision in the ACCESS Act requiring foreign companies to respect user privacy and cybersecurity amounts to little more than wishful thinking.

Furthermore, the legislation ignores the central role that data collection and analysis plays in China's long-term strategy. In 2020, China's National Development and Reform Commission defined data as the fifth factor of production for China's economy,[63] and China is reportedly executing a centrally-directed systematic plan to harvest data on U.S. companies, individuals, and the U.S. government.[64] The U.S. legislative proposals would effectively require large U.S. technology companies to assist China and other foreign governments in pursuing these goals – while undermining U.S. citizens' privacy and cybersecurity.

C. Risk of Foreign Influence and Cybersecurity Vulnerabilities

The so-called "non-discrimination" provisions of the ACIOA/AICOA would require large U.S. technology companies to treat third-party products, services, and businesses on a par with their own – even if the relevant third parties spread foreign influence, generate content that is spammy, or pose a cybersecurity threat to U.S. citizens. For example, under the legislation, large U.S. technology companies such as Facebook, Google, and Apple would have to present apps, e-commerce listings, and search results from foreign companies such as Alibaba, Tencent, and ByteDance with equal prominence as those of any other companies. Similarly, large U.S. technology companies would be barred from deprioritizing state-owned foreign media sources such as the Russian network RT and the Chinese network CGTN.

In addition, large U.S. technology companies would be barred from employing their own security-related products and services to ensure the integrity and security of their platforms and protect users. For example, if such companies pre-install proprietary anti-virus/cybersecurity software designed to safeguard user data, this could potentially violate the legislation's non-discrimination provisions.

As noted above, the text of the ACIOA/AICOA recognizes the risks to cybersecurity and privacy and seeks to mitigate the risk with an affirmative defense. However, the defense is so narrow that it is unlikely to be accessible in practice.

---

[62] ACCESS Act, § 3(b)(1).

[63] *See* Ouyang Shijia & Chen Jia, "New guideline to better allocate production factors," CHINA DAILY (Apr. 10, 2020). The other four factors of production are land, labor, capital, and technology. *See id.*

[64] The National Security Commission on Artificial Intelligence, Final Report (Mar. 2021) at 25, 49.

Specifically, the ACIOA's prohibitions on discriminatory conduct would not apply if the "covered platform" establishes, by clear and convincing evidence, that the relevant conduct would not harm the competitive process by restricting or impeding legitimate activity by business users; or was narrowly tailored and could not be achieved through a less discriminatory means, was nonpretextual, and was necessary to: (i) prevent a violation, or comply with, federal or state law, or (ii) protect user privacy or other non-public data. The AICOA contains a similar affirmative defense, although there are nuanced differences, including the replacement of the "clear and convincing" standard with a "preponderance of the evidence" standard and quantifying that the action was "reasonably" necessary.[65] Given the fact that companies would have the burden of establishing the defense, the multiple conditions on the defense, uncertainty about how enforcement agencies and U.S. courts would interpret the conditions, and the practical difficulty and administrative burdens associated with establishing that the affirmative defense should apply in any particular instance, companies would be unlikely to rely on it in the normal course. Instead, the legislation would pressure them to adhere to the non-discrimination provisions of the ACIOA/AICOA, even if doing so undermines cybersecurity.

Thus, the proposed legislation would thwart U.S. technology companies' efforts to weed out bad products, services, information, and security risks – creating a multitude of opportunities for bad actors to mislead or attack those who use the products and services that they provide. Meanwhile, foreign companies would generally remain unaffected – and thus could continue to deprioritize spammy, misleading, and insecure products and services. The net effect would be to drive U.S. consumers to switch to different technology platforms – not to stop the business practices targeted by the legislation.

D. Absence of Countervailing Benefits for U.S. Consumers

NERA, an economic consulting firm, has estimated that the welfare effects of the U.S. legislative proposals would be negative $300 billion.[66] This large cost represents the inefficiencies resulting from undoing the integration of large technology companies. Mergers can create synergies that benefit consumers, and conversely forced reductions in scale create cost inefficiencies.

Moreover, the various types of business conduct that the U.S. legislation seeks to address – such as the prevalence of large technology companies; acquisitions of smaller companies to prevent future competitors from emerging; and technology platforms preferencing their own products, services, and lines of business – would all

[65] AICOA, § 2(d).

[66] *See* Christian M. Dippon & Matthew D. Hoelle, *The Economic Costs of Structural Separation, Line of Business Restrictions and Common Carrier Regulation of Online Platforms and Marketplaces: A Conceptual Assessment*, NERA Economic Consulting (Oct. 20, 2021) at 13, 15.

persist even if the legislation were adopted. While covered platforms would be barred from engaging in such conduct, other companies would still be able to do so, including large foreign companies such as Chinese behemoths, which have fewer U.S. users and therefore would not qualify as "covered platforms."

Thus, while the legislation would impose significant costs on those companies that qualify as "covered platforms," consumers would continue to encounter the same types of practices that the legislation is designed to address. It is therefore unclear how consumers will benefit, while the risks to consumer welfare – as well as national security – are substantial.

IV. Conclusion

American prosperity and national security in the 21st century will depend on how the U.S. Government responds to China, the EU, and other governments seeking to dominate the technologies of the future. Foreign companies will continue to benefit from aggressive industrial policies that skew the competitive landscape in their favor – including through competition law, generous industrial subsidies, market access restrictions, distorted IP regimes, onerous data security regimes that keep competitors at bay, and in some cases, absence of rule of law. The United States must develop an urgent response that meet this challenge, without sacrificing our values or the system of free enterprise that has made the U.S. economy the world's most dynamic and innovative.

In addition to foreign efforts targeting U.S. companies, antitrust proposals under consideration in Congress would run directly counter to this goal and undermine the development of much-needed U.S. responses to foreign competitive threats to economic and national security. Instead of making the United States more innovative and more competitive globally, they would hamstring and even dismantle America's strongest technology companies. Simultaneously, the proposals would clear the way for foreign companies from China, Russia, and the EU to become more prominent, both in the U.S. market and globally – ushering greater foreign influence into the U.S. market. Such measures would undermine U.S. national security and expose U.S. citizens to greater privacy and cybersecurity risks, in the name of countering monopolistic behavior.

Congress should reject these legislative proposals and consider embarking on the following path:

- **Operate on the overarching principle of "do no harm."** Congress should avoid giving license to foreign jurisdictions that are targeting the hard-won comparative advantage of U.S. firms. Legislation that is under consideration would amplify and excuse the mounting harm being done to the

competitiveness of U.S. companies, who are critical to the United States and its ability to compete effectively against non-market and authoritarian regimes in the 21st century economy.

- **Market capitalization should not be a legislative or regulatory trigger for targeting companies.** Market capitalization is a measure of future confidence in the performance of a company, not just domestically, but globally. U.S. companies with large and growing market capitalizations reach their size based on their value to markets around the world. This is a projection of American competitiveness as well as an important sign of international leadership. Further, reliance on market cap as a trigger, even when indexed for inflation, will result in additional American companies being captured as market capitalizations rise and fall independent of inflation. A one-size-fits-all approach will result in unintended and harmful outcome to the U.S. economy

- **Adopt narrowly tailored responses to well-documented digital economy concerns through targeted regulation, not changing antitrust laws or targeting particular companies.** The suggested legislation lumps together companies with distinctly different business models to universally respond to a collection of concerns that aren't appropriately applicable to each of the companies captured. Completing work on a federal privacy law would be one example of where a targeted legislative response to a digital economy challenge should be a priority focus of Congressional efforts.

- **Address rapidly accelerating market distortions that arise from non-market economies, including excessive concentrations under State ownership and influence.** Antitrust law in the United States is rooted in market economics and enforced against private sector restraints of trade, not government restraints to promote national champions, restrain the growth opportunities of foreign-based competitors, and compel technology transfer. Our antitrust laws are currently ill-equipped to address such an approach. Congress should bolster the U.S. government's toolkit in combatting NME practices globally.

- **Institute regular briefings from the U.S. national security community to committees on how China's approach to antitrust, data, standards and technology development and acquisition policies impacts U.S. competitiveness, innovation, and national security.** These briefings should specifically include Congressional committees that do not regularly receive them (e.g., Senate and House Judiciary, Senate Finance and House Ways and Means, Senate Banking and House Financial Services, Senate and House Commerce). Such briefings for Senate and House members are critical to help

ensure that legislation is not developed in a vacuum and appropriately considers the broader context of intensifying competition with China.

If adopted, these recommendations would avoid self-harm in the effort to ensure the United States remains competitive and well placed to maintain its national security posture.

ANNEX

I. U.S. Legislative Proposals Would Radically Distort Antitrust Law to Single Out a Small Group of Large and Globally Competitive U.S. Technology Companies

In 2021, members of both houses of Congress introduced a raft of antitrust-related bills targeting large U.S. technology companies. The ostensible purpose of these bills is to promote competition in the tech sector. In fact, however,, the legislation would punish aggressive competition on the merits, and would have a wide range of further unintended consequences – dampening U.S. innovation and weakening the U.S. innovation ecosystem; providing a competitive advantage to foreign rivals; facilitating the spread of foreign influence and misinformation within the United States; and undermining the cybersecurity of U.S. technology services. Meanwhile, the legislation would not impose any constraints on the foreign rivals of large U.S. technology firms, because for the foreseeable future they would not meet the statutory definitions of "covered platforms."

The bills at issue include several in a package approved by the House Judiciary Committee in June: the American Choice and Innovation Online Act ("ACIOA"); the Ending Platform Monopolies Act; the Platform Competition and Opportunity Act; and the Augmenting Compatibility and Competition by Enabling Service Switching ("ACCESS") Act.[67] In August 2021, the Open Aps Market Act was introduced in the House and the Senate.[68] In addition, in October 2021, Senators Amy Klobuchar, Chair of the Subcommittee on Competition Policy, Antitrust, and Consumer Rights, and Chuck Grassley, Ranking Member of the Judiciary Committee, introduced a bill that is similar to the ACIOA, entitled the American Innovation and Choice Online Act ("AICOA").[69] And in November 2021, Senators Klobuchar and Tom Cotton introduced the Platform Competition and Opportunity Act, a companion to the House bill of the

[67] American Choice and Innovation Online Act (ACIOA), H.R. 3816 § 2(g)(4), 117th Cong. (2021); Ending Platform Monopolies Act, H.R. 3825 § 5(5), 117th Cong. (2021); Platform Competition and Opportunity Act, H.R. 3826 § 3(d), 117th Cong. (2021); Augmenting Compatibility and Competition by Enabling Service Switching Act, H.R. 3849 § 5(6), 117th Cong. (2021).
[68] S. 2710, H.R. 5017, 117th Cong. (2021).
[69] S. 2992, 117th Cong. (2021).

same name.[70] Several other antitrust-related bills have been introduced in 2021 as well.[71]

Together, these bills represent a radical departure from modern principles of antitrust law, which focuses primarily on consumer welfare. As the Supreme Court has stated, "Congress designated the Sherman Act as a 'consumer welfare prescription.'"[72] Accordingly, antitrust enforcement agencies generally administer U.S. antitrust laws to ensure that anticompetitive conduct does not reduce consumer welfare – for example, by enabling monopolistic pricing to consumers and cartel activity. By contrast, the proposed legislation would regulate U.S. companies based on rigid quantitative thresholds and target wholesale categories of conduct on an *ex ante* basis, with no requirement to demonstrate harm to competition or negative effects on consumer welfare. Several influential voices within the Biden Administration appear to support such an approach, including the current Chair of the Federal Trade Commission (FTC),[73] but the Administration as a whole has not taken an official position on the legislation.

A. Scope of Application: The Legislation Would Apply Only to a Small Group of Large U.S. Technology Firms, Leaving Foreign Companies Unaffected

The bills listed above would apply only to operators of a "covered platform," defined as a company which, over the preceding 12 months, (i) has 50 million U.S.-based monthly active users or 100,000 U.S.-based monthly active business users, (ii) has a market cap of either more than $550 or $600 billion, and (iii) is a "critical trading partner for the sale or provision of any product or services offered on or directly related to the online platform."[74] A "critical trading partner," as defined in the proposals, has the ability to restrict or impede (i) "the access of a business user to its users or customers," or (ii) "the access of a business user to a tool or service that it needs to effectively serve its users or customers."[75] If these criteria are met, then the FTC and the Department of Justice's Antitrust Division (DOJ) must designate the

---

[70] Platform Competition and Opportunity Act, S. 3197, 117th Cong. (2021).

[71] *See, e.g.*, Tougher Enforcement Against Monopolies ("TEAM") Act, S. 2039, 117th Cong. (2021) (introduced by Senators Chuck Grassley and Mike Lee); Senator Josh Hawley's Trust-Busting for the Twenty-First Century Act and Bust Up Big Tech Act (S. 1074 and S. 1204, respectively, 117th Congress (2021)).

[72] Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979).

[73] *See, e.g.*, David McLaughlin, *Senate Confirms Google Foe as DOJ's Antitrust Chief*, Bloomberg (Nov. 16, 2021); Cecilia Kang, *A Leading Critic of Big Tech Will Join the White House*, N.Y. Times (Mar. 5, 2021).

[74] H.R. 3816, § 2(g)(4); H.R. 3825, § 5(5); H.R. 3826, § 3(d); H.R. 3849 § 5(6). The AICOA sets $550 billion rather than $600 billion as the monetary threshold for criterion (ii). *See* S. 2992, § 2(h)(4)(B)(ii). And the Senate Platform Competition and Opportunity Act only sets the market capitalization threshold at the time of enactment of the statute, *not* during the preceding 12 months. *See* S. 3197, § 3(d)(2)(B).

[75] H.R. 3816 § 2(g)(6); H.R. 3825 § 5(7); H.R. 3826 § 3(f); H.R. 3849 § 5(8).

digital platform as a "covered platform."[76] This limited definition appears to encompass only the following digital platforms: Google, Amazon, Facebook, Microsoft, and Apple.[77] It would also apply to U.S. companies that become similarly successful in the future. It also appears that, at most, only a few foreign firms would currently meet the thresholds to qualify as a "covered platform."[78]

Because the legislation applies to operators of covered platforms, and not to specific business lines, it would sweep in a range of activities that are not the intended targets of the legislation. For example, although the legislation may target Amazon for its retail platform, and Microsoft for its social media company LinkedIn and its search engine Bing, the legislation would impose significant new burdens on the enterprise-facing cloud services units of both companies (Amazon Web Services and Microsoft Azure). Another unintended consequence is that companies near the threshold to qualify as "covered platforms" would have a strong incentive to manage their market capitalization and/or number of U.S. users to avoid being covered by the legislation.

At present, only a handful of U.S. technology companies currently meet the definition of a "covered platform" (as noted above). However, according to a report by the economic consulting firm NERA, at least 13 U.S. companies that are not principally technology companies, may meet the thresholds within 7 to 10 years.[79] Thus, the antitrust legislation would potentially have wide-ranging implications for companies in a variety of sectors, including entertainment, banking, retail, investment, and payment services – forcing them to break up and constraining their operations, apparently as an unintended consequence.

B. The Legislation Would Drastically Constrain How "Covered Platforms" Do Business

[76] H.R. 3816 § 2(d); H.R. 3825 § 6(a); H.R. 3826 § 4(a); H.R. 3849 § 6(a).
[77] The monthly active user or monthly active business user thresholds are too large, as currently drafted, to encompass other tech companies, such as Twitter, Netflix, and others. *See* Aurelien Portuese, "The House's Antitrust Legislative Package: An Innovation Perspective" (ITIF Aug. 2021).
[78] We are aware of only one example of a foreign digital platform with more than 50 million U.S. users: TikTok. However, TikTok's parent company, ByteDance, does not meet the applicable market capitalization threshold of $600 million (or $550 million in the AICOA). *See TikTok Statistics – Updated Sep 2021*, Wallaroo (Sept. 27, 2021); Brady Ng, *TikTok Creator ByteDance Hits $425bn Valuation on Gray Market*, Nikkei Asia (June 26, 2021).
[79] The 13 companies are: Berkshire Hathaway, Walmart, Home Depot, Comcast, AT&T, Visa, Mastercard, Walt Disney, Netflix, JP Morgan Chase, PayPal, Bank of America, and Cisco. Christian M. Dippon & Matthew D. Hoelle, *The Economic Costs of Structural Separation, Line of Business Restrictions and Common Carrier Regulation of Online Platforms and Marketplaces: A Conceptual Assessment*, NERA Economic Consulting (Oct. 20, 2021) at 8.

The legislation would:

- **Break up large U.S. technology companies**

The Ending Platform Monopolies Act would prohibit covered platforms from owning or controlling any other line of business that (i) uses the platform to sell its products or services, (ii) offers a product or service that platform users are required to purchase for "preferred status or placement" on the platform, or (iii) creates an incentive or ability for the platform to advantage its own business or disadvantage[80] a competing business.[81] The FTC and DOJ would have the power to force any company that violates this rule to divest.[82]

Thus, if adopted, the legislation would require large U.S. technology companies to divest their various businesses – until they either no longer qualify as covered platforms, for example because the number of U.S. users or market capitalization drops below the threshold level; or they divest all businesses that sell, advertise, or otherwise promote their own goods and services on the covered platform. The companies to be divested could include, for example, digital marketplaces, online video streaming services, search engines, app stores, and so on. However, foreign technology competitors would not be subject to the requirement to divest because they do not qualify as covered platforms. Thus, the bills would create significant buying opportunities for foreign companies to acquire the divested companies at a discount.

- **Prohibit large U.S. technology companies from engaging in significant new acquisitions or investments**

The Platform Competition and Opportunity Act would presumptively prohibit covered platforms from engaging in any acquisition or investment valued at over $50 million, unless the platform can demonstrate by "clear and convincing evidence" that the target is not a competitor, a nascent or potential competitor, or any other company that would "enhance or increase" the covered platform's market position or ability to retain its market position.[83] In essence, the bill would prohibit covered platforms from engaging in horizontal as well as vertical mergers – even if such combinations do not reduce competition or can increase efficiencies and serve the

[80] Notably, "disadvantage" is not defined in the bill.
[81] H.R. 3825 § 2(b).
[82] *See* 15 U.S.C. § 41, et seq.; 15 U.S.C. § 12, et seq. This piece of legislation has, appropriately, been dubbed the "break up" bill. Competition law experts have expressed caution about the prudence of breaking up large technology companies. *See, e.g.*, Eleanor Fox & Don Baker, "Antitrust and Big Tech Breakups: Piercing the Popular Myths by Cautious Inquiry," Competition Policy International (Oct. 25, 2021).
[83] *Id.* § 2(b).

interests of consumers. Furthermore, because this rule would apply only to "covered platforms," it would leave foreign companies unaffected.

This provision could have a wide range of unintended consequences. First and foremost, it would likely discourage entrepreneurship. In general, being acquired is the main way that U.S. startups expect to achieve financial success. Data from 2020 indicate that 58% of startups expect to be acquired – and this is a strong incentive to make the investments necessary to start the company up in the first place.[84] By barring the largest U.S. technology companies from engaging in acquisitions, the legislation would weaken the U.S. innovation ecosystem as a whole. In addition, it would once again create buying opportunities for foreign companies– in effect transferring significant innovative assets from U.S. to foreign hands.

The provision is also overbroad in important ways. While it is ostensibly intended to prevent future anticompetitive conduct, it would also bar acquisitions that are pro-competitive and pro-consumer. For example, large U.S. technology companies may want to acquire companies that perform important cybersecurity functions, so as to disseminate cybersecurity expertise throughout their organization. Similarly, such technology companies may want to acquire companies that specialize in preventing spam from reaching consumers. The legislation would prohibit such transactions, to the detriment of consumers.

- **Require large U.S. technology companies to disclose user data to competitors – including those that are foreign-controlled**

The ACIOA would make it unlawful for covered platforms to "restrict or impede a business user from accessing data generated on the platform by the activities of the business user or its customers through an interaction with the business user's products or services." The AICOA contains a similar provision (modified by a manager's amendment, discussed previously).[85] In addition, under the mantle of "interoperability," the ACCESS Act would mandate that covered platforms maintain "transparent, third party-accessible interfaces" to enable the transfer of user data to competing or potentially competing businesses.[86]

[84] *See* Jeff Farrah, "Restrictions on acquisitions would stifle the US startup ecosystem, not rein in big tech," TechCrunch (May 19, 2021).
[85] Making it unlawful to "materially restrict or impede a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the business user's products or services." § 2(b)(4).
[86] The bill provides: "A business user shall not collect, use, or share the data of a user on a covered platform except for the purposes of safeguarding and security of such data or maintaining interoperability of services." § 4(f)(2).

Thus, these bills would require large U.S. technology companies to provide user data, including data generated through business interactions with U.S. citizens, to any other company upon request, whether U.S. or foreign. The bills would also require such companies to create the technical infrastructure to facilitate the transfer of such user data to any other company on request – even if the requestor is located outside the United States. This requirement goes far beyond merely ensuring that consumers have a practical way to switch between various technology platforms and online services. Covered platforms would be required to provide the relevant information to other businesses, even if consumers have no interest in switching.

The ACCESS Act appears to recognize that these measures pose a significant risk to the security of individuals' private data. Accordingly, the ACCESS Act contains a provision on data security that states: "A competing business or a potential competing business that receives ported user data from a covered platform shall reasonably secure any user data it acquires, and shall take reasonable steps to avoid introducing security risks to data or the covered platform's information systems."[87] This provision may require companies receiving ported user data to impose data security measures. However, the duplication and proliferation of an individual user's data increase the risk that it will be compromised, even if U.S. law requires companies receiving the data to take appropriate precautions. Furthermore, the ACCESS Act does not address situations where foreign governments ask companies that receive ported data to turn it over. For example, Chinese law requires companies to hand over data to Chinese government authorities upon request to facilitate law enforcement and national security activity.[88] Such data transfers appear to be permissible under the ACCESS Act. As a result, the ACCESS Act could potentially result in U.S. citizens' data being used for the Chinese or other foreign government's law enforcement purposes – for example, to identify and apprehend individuals who support political or human rights causes that China considers threatening.

- **Require large U.S. technology companies to treat third-party products, services, and businesses on a par with their own – even if this leads to increased foreign influence or misinformation, or compromises cybersecurity**

The ACIOA and AICOA prohibit what they term "discriminatory" conduct by covered platforms. Specifically, they prohibit covered platforms from (i) advantaging/preferencing the covered platform operator's own products, services, or

[87] § 3(b)(1).

[88] Article 28 of China's Cybersecurity Law [Zhonghua renmin gongheguo wangluo anquanfa] (2016) calls upon network operators to provide technical support and assistance to public security, *i.e.*, law enforcement, and national security authorities, in the investigation of criminal activity.

lines of business over those of another business user;[89] (2) excluding or disadvantaging the products, services, or lines of business of another business user relative to the covered platform operator's own products, services, or lines of business; or (3) discriminating among similarly situated business users. The AICOA contains similar provisions.[90] The ACIOA also bans a range of other conduct that it deems discriminatory. The ACIOA would be enforceable not only by the FTC and DOJ but also through private lawsuits that can be brought by persons or companies injured by conduct that the ACIOA prohibits.[91]

The ACIOA/AICOA would include a very narrow "affirmative defense" which – if covered platforms can satisfy it – would allow them to derogate from the non-discrimination requirements. Specifically, the ACIOA's prohibitions on discriminatory conduct would not apply if the covered platform establishes, by clear and convincing evidence, that the relevant conduct would not harm the competitive process by restricting or impeding legitimate activity by business users; or was narrowly tailored and could not be achieved through a less discriminatory means, was nonpretextual, and was necessary to: (i) prevent a violation, or comply with, federal or state law, or (ii) protect user privacy or other non-public data. Covered platforms would have the burden of establishing that they qualify for the affirmative defense, and in practice it would be up to U.S. courts to adjudicate whether the defense applies. The AICOA contains a similar affirmative defense, although there are nuanced differences, including the replacement of the "clear and convincing" standard with a "preponderance of the evidence" standard.[92] Given the multiple conditions on the affirmative defense, uncertainty about how enforcement agencies and U.S. courts would interpret the conditions, and the practical difficulty and administrative burdens associated with establishing that the affirmative defense should apply in any particular instance, the utility of the affirmative defense is likely to be limited in practice.

The non-discrimination provisions of the ACIOA/AICOA would likely result in greater prominence for apps, e-commerce listings, and search results provided by foreign companies such as Alibaba, Tencent, and ByteDance on U.S. platforms. This is because covered platforms would be barred from deprioritizing the products, services, and lines of business of such foreign companies. The non-discrimination provisions would also boost products and services that covered platforms might currently weed out for reasons related to public welfare. Examples include the

[89] "Advantaging" is the operative phrase in the relevant provision of the ACIOA, and "unfairly preference" is the operative phrase in the relevant provision of the AICOA. § 2(a)(1).
[90] Whereas the ACIOA prohibits "*advantaging* the covered platform operator's own products, services, or lines of business over those of another business user," the ACIOA prohibits "*preferenc[ing]*" such products, services, or lines of business. § 2(a)(1).
[91] This is discussed in the following section.
[92] AICOA, § 2(d).

Russian television network RT and the Chinese network China Global Television Network (CGTN), other sources of disinformation and radical ideologies, and "spammy" sources of information.

The non-discrimination provisions of the ACIOA/AICOA would likely compromise cybersecurity as well. Large U.S. technology companies currently promote certain products and services (whether their own or those of other companies) because they exemplify good security practices. Similarly, large U.S. technology companies currently exclude products and services from their platforms that they consider harmful. However, the ACIOA/AICOA would generally prohibit such security-related practices as "discriminatory" – and moreover, would subject the targets to massive civil penalties if a court decides that a technical fix could have been more narrowly tailored (as discussed in the following section). Although the affirmative defense appears intended in part to mitigate this risk, as noted above its utility is likely to be extremely limited in practice.

- **Create a private right of action that enables companies, including foreign companies, to sue "covered platforms" that deprioritize their products, services, or lines of business**

The ACIOA would create a private right of action so that persons (including companies) that are injured as a result of a violation of the legislation's so-called non-discrimination provisions may recover monetary damages or an injunction.[93] Thus, for example, if a covered platform were to deprioritize news from RT or CGTN, or from a source of a radical ideology, the person or business that is the source of the information could sue the covered platform either to recover monetary damages or obtain injunctive relief. In practical terms, this private right of action is likely to increase pressure on covered platforms to comply strictly with the ACIOA's nondiscrimination provisions. In addition, plaintiffs would be able to recover damages even in instances where the violation of the ACIOA is inadvertent.

- **Impose substantial civil penalties, even for first-time offenses.**

The ACIOA would impose a remedy of up to the greater of 15% of U.S. revenue in the previous calendar year or 30% of the U.S. revenue of the impacted company's business line during the time the violation occurred,[94] while the AICOA would allow for a remedy of up to 15% of the total U.S. revenue of the offending company during the time the violation occurred.[95] For repeat offenders, the ACIOA instructs courts to consider requiring the company's Chief Executive Officer to forfeit compensation

[93] In addition, the Bust Up Big Tech Act would also create a private right of action so that any person injured by a violation of the act could sue and recover up to $1 million per violation. *See* S. 1204 § 2(e).
[94] *See* ACIOA, § 2(f)(1).
[95] *See* AICOA, § 2(g)(1).

received during the preceding 12 months.[96] The AICOA goes a step further and suggests that additional corporate officers "as appropriate to deter violations" should also be required to forfeit their earnings.[97]

C. China Is Pursuing a Comprehensive Regulatory Agenda to Dominate Technologies of the Future While Constraining U.S. Technology Companies

China's regulatory apparatus is geared in substantial part to achieve industrial policy goals and, in particular, China's economic, technological, and national security advancement. Indeed, China's 14th Five-year Plan (2021-2025)[98] declares that it is a national security objective for China to dominate next-generation technologies.[99] China's legal and regulatory apparatus is designated and empowered to promote this objective.

One significant expression of China's techno-nationalist regulatory agenda is the Anti-Monopoly Law ("AML"), China's competition law. Unlike antitrust law in the United States, the AML is not merely a tool to promote consumer welfare. Rather, China also uses the AML to encourage the growth and technological advancement of Chinese state-owned enterprises ("SOEs") and national champions – both within China and, especially, overseas.[100] The U.S. Chamber of Commerce issued a detailed report on China's use of its antitrust law as a tool of industrial policy in 2014, and enumerated concerns have only intensified in recent years. Today, Chinese companies – whether state-owned, state-influenced, or even private – effectively serve at least in part as instruments of the Communist Party (CCP) to increase China's global power. By the same token, China uses the AML to limit the competitiveness of foreign companies within China and to pressure or compel them to transfer technology to Chinese companies. While China also uses the AML to serve consumer

---

[96] *See* ACIOA, § 2(f)(3).
[97] *See* AICOA, § 2(g)(3).
[98] *See* Outline of the People's Republic of China, 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, XINHUA (Mar. 12, 2021) [Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisi ge wu nian guihua he 2035 nian yuanjing mubiao gangyao]
[99] Outline of the People's Republic of China, 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, XINHUA (Mar. 12, 2021) [Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisi ge wu nian guihua he 2035 nian yuanjing mubiao gangyao]; *see also* Rush Doshi, THE LONG GAME (2021) at 288 ("China is pursuing a robust, state-backed effort to dominate these technologies [of the Fourth Industrial Revolution] and to use them to erode various American advantages.").
[100] Central SOEs enjoy a limited exemption under Article 7, and combinations between SOEs are not subject to merger review because the parties are under common ownership.

welfare-related policy objectives, it subordinates these goals to the broader goals of national economic development and global dominance.

Beyond the AML, China uses a wide array of legal and policy tools to ensure that SOEs and national champions have preferential access to the Chinese home market and expand aggressively overseas. These include subsidies for favored Chinese companies, including in relation to overseas investment in connection with the Belt and Road Initiative, which advances Chinese investment and trade in developing countries; restrictions on foreign services and investment in the technology sector; an onerous and increasingly complex legal regime governing data and privacy; and a CCP-dominated judiciary biased in favor of the transfer of foreign technology to Chinese companies.

2021 was marked by many new developments related to China's regulation of the technology sector, including: more vigorous enforcement with respect to China's own technology companies as part of a broader regulatory effort to rein them in (the so-called "tech crackdown"); recently announced plans to promote the director of the Anti-Monopoly Bureau within the State Administration for Market Regulation (SAMR) to the deputy ministerial level in the newly-elevated National Anti-Monopoly Bureau;[101] a plan to significantly increase the number of personnel in SAMR who are dedicated to AML enforcement; proposed amendments to the text of the AML; the issuance of new draft guidelines on "super platforms," similar in broad outlines to the U.S. and EU legislation discussed throughout this report; the issuance of the Data Security Law (effective September 2021) and the Personal Information Protection Law (effective November 2021); and the release of a sweeping, first-of-its kind regulation on the use of algorithmic recommendations.[102] These changes constitute an intensification of preexisting trends in AML enforcement – namely, the Chinese government's reliance on competition law to advance industrial policy goals that are often unrelated to consumer welfare. The "tech crackdown", in particular, is part of a CCP-led campaign to make clear that the Party leads in all aspects of Chinese society.[103] There is no indication that this will lessen China's industrial policy interest in other domains, such as strengthening SOEs and national champions to compete effectively in China and worldwide; as well as ensuring that such companies are at the forefront of the most important technologies of the future.

---

[101] *See* "China's State Council appoints new supervisor of anti-monopoly regulator," GLOBAL TIMES (Nov. 15, 2021).

[102] Internet Information Service Algorithmic Recommendation Management Provisions [Hulianwang xinxi fuwu suanfa tuijian guanli guiding] (Opinion-Seeking Draft) Aug. 27, 2021.

[103] *See, e.g.*, Charles Mok, "More than a Tech Crackdown, It's Farewell to China's Economic Reform," FRIEDRICH NAUMANN FOUNDATION FOR FREEDOM (Aug. 20, 2021); Charlie Campbell, *Here's What the Crackdown on China's Big Tech Firms Is Really About*, TIME (July 13, 2021).

II. Industrial Policy, Including Techno-Nationalism, Drives Competition Law Enforcement in China

Both the AML and China's broader competition policy are oriented around supporting Chinese companies, as outlined in the Chamber's 2014 report entitled *Competing Interests in China's Competition Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy*.[104] Below, we provide a brief overview of the types of AML enforcement that China uses for a variety of industrial policy purposes, including the promotion of Chinese companies and industries in strategic sectors such as semiconductors – while also discriminating against U.S. companies.

A. Merger reviews

SAMR (and its predecessor agency for merger reviews, the Anti-Monopoly Bureau in China's Ministry of Commerce ("MOFCOM")) is prone to conduct merger reviews in two ways that advance industrial policy objectives in industries of importance to China: first, it may withhold approval in foreign-related merger reviews until the foreign company agrees to concessions that will erode its advantages over Chinese competitors; and second, it may impose conditions for approval of foreign-related transactions that benefit Chinese companies and place their foreign companies at a competitive disadvantage. Mergers of state-owned enterprises, regardless of their market share, controlled by the central government are exempt from merger review by virtue of their common ownership.[105] This pattern is especially pronounced for companies operating in sectors that China has deemed strategic, such as semiconductors, aviation, and military equipment.[106]

Examples of the use of merger reviews to promote industrial policy objectives include:

- Imposing "hold-separate" orders to keep merging foreign entities separate for several years, giving Chinese companies time to "catch up"

[104] *See* "Competing Interests in China's Competition Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy," U.S. CHAMBER OF COMMERCE (2014).
[105] Article 7 of the AML; *see also* Keith Zhai, "China Set to Create New State-Owned Rare-Earths Giant," THE WALL STREET JOURNAL (Dec. 3, 2021).
[106] As context, it is important to note that China's competition law authority approves the vast majority of M&A transactions without imposing any conditions – but nearly all cases where approval is conditional (*i.e.*, remedies are imposed) have involved foreign companies. In other words, of the 25 transactions conditionally approved by SAMR or MOFCOM since 2015, 25 involved foreign companies. Moreover, the protection of consumer rationale was a stated objective in only 2 of the 25 cases (involving eyeglass retailers and medical service providers). In the majority of cases, SAMR/MOFCOM instead cited potential harm to Chinese competitor companies or downstream entities and increased barriers to entry as rationales for imposing conditions that dull the impact of the transaction.

before the combined entity can realize the benefits of its union.[107] SAMR/MOFCOM have applied such orders in transactions involving strategic industries such as disk drives, optical communications devices and semiconductors. Such "hold-separate" behavioral orders are not typically imposed by U.S. or European regulators.[108]

- Ordering the merged entity to share intellectual property with Chinese companies or otherwise support R&D efforts in China.[109] In effect, this constitutes a form of technology transfer by government compulsion or pressure.
- Requiring the merged entity to ensure continuous supply and access to technology for Chinese downstream companies, as a condition for completing the merger.[110] Such conditions are intended to strengthen the Chinese companies to which the products, services, or technology are provided.
- Withholding or delaying approval of the merger or acquisition in order to give Chinese companies greater opportunity and leverage to acquire

---

[107] *See* John Ratliff, Frédéric Louis and Cormac O'Daly, "International Merger Remedies," THE MERGER CONTROL REVIEW (7th ed. 2016) at 52 ("hold separate remedies are not usual in the US and the EU, mainly because authorities favour clear-cut structural remedies"); *see also* "SPIL/ASE's wrestle with MOFCOM rolls on," PARR (Sept. 8, 2017) (explaining that MOFCOM's review process of the two semiconductor manufacturers may be help China's top semiconductor manufacturer in "catching up … in terms of market share").

[108] *See* John Ratliff, Frédéric Louis and Cormac O'Daly, "International Merger Remedies," THE MERGER CONTROL REVIEW (7th ed. 2016) at 52 ("hold separate remedies are not usual in the US and the EU, mainly because authorities favour clear-cut structural remedies"); *see also* "SPIL/ASE's wrestle with MOFCOM rolls on," PARR (Sept. 8, 2017) (explaining that MOFCOM's review process of the two semiconductor manufacturers may be help China's top semiconductor manufacturer in "catching up … in terms of market share").

[109] One of the conditions of MOFCOM's approval of the Bayer-Monsanto merger was for the combined entity to give Chinese agricultural application developers access to Bayer's proprietary digital agriculture platform. *See* "MOFCOM Announcement No. 31 of 2018 on Decisions from Anti-Monopoly Review of the Concentration of Undertakings on Conditional Approval of Proposed Acquisition of Equity in Monsanto by Bayer," MOFCOM (Mar. 13, 2018); *see also* "Bayer, Monsanto deal wins conditional antitrust clearance in China," MLEX (Mar. 29, 2018). In 2018, SAMR approved the tie-up of U.S. companies Rockwell Collins and United Technologies so long as the combined entity continued to "invest in R&D and innovation activities in China to help advance development of China's aviation industry." *See* "SAMR Announcement on Decisions from Anti-Monopoly Review on Conditional Approval of Proposed Acquisition of Equity in Rockwell Collins by United Technologies," SAMR (Nov. 23, 2018); *see also* "United Technologies secures antitrust approval in China for Rockwell Collins deal, with conditions," MLEX (Jan. 8, 2019).

[110] *See, e.g.*, "SAMR Announcement on Decisions from Anti-Monopoly Review on Conditional Approval of Proposed Acquisition of Certain Business of TTS by Cargotec," SAMR (July 5, 2019); *see also* "SAMR's decision on TTS/Cargotec reflects export control impacting China's merger review," PARR (July 22, 2019) (explaining that SAMR's conditional approval decision emphasized that for five years the merged entity "cannot maliciously delay the supply of products without any justifiable reason" and that this "stable supply" remedy was described in stronger terms than similar decisions in the past).

assets that SAMR requires to be divested.[111] In such cases, the Chinese acquirers of the divested assets are not parties to the transaction under review. Thus, in effect, the conditions imposed by SAMR bolster the competitive position of Chinese parties that are not party to the actual transaction.

- Withholding and delaying approval of the merger or acquisition or merger to the point that the parties decide to call the deal off or are deterred from pursuing a deal.[112]

Furthermore, even if delays from Chinese antitrust regulators do not lead to terminated deals, they raise the cost of doing business for affected U.S. companies, which reportedly must overpay for potential deal partners to bear the risk that Chinese antitrust regulators may subject such deals involving U.S. companies in strategically important industries to prolonged merger reviews.[113]

B. Abuse of dominance investigations

Historically, China's competition law authorities have used abuse of dominance investigations to target foreign companies in an overt and seemingly lawless manner. For example, as of 2013, the National Development and Reform Commission (NDRC), one of SAMR's predecessors, pressured companies to confess to AML violations or face much more severe sanctions, and in at least one instance the NDRC casually threatened to initiate investigations against more than a dozen foreign companies at

[111] For example, MOFCOM's review of the Bayer-Monsanto merger took over a year, and while China and regulators in other countries ordered the companies to divest many of their business lines as a condition of approval, and a prolonged merger review generally drives down the price of these assets. China's CITIC Agri Fund and China's sovereign wealth fund had teamed up to bid for the assets in China to be divested. *See* "Monsanto/Bayer remedy asset bidder China CITIC Agri Funds drop out – sources," PARR (July 13, 2017).

[112] This was the case in Qualcomm's failed acquisition of Dutch-American semiconductor manufacturer NXP, which had been under SAMR's merger review for approximately 450 days before the parties terminated the deal. Contemporaneous media reports indicate that merger reviewers withheld approval, at least in part as a reaction to bilateral trade tensions in 2018. In addition, in 2021, another semiconductor transaction was called off after U.S.-based Applied Materials terminated its agreement to acquire Japan's Kokusai Electric after waiting more than 500 days for approval from SAMR. In 2016, similar delays motivated by political and/or industrial policy concerns are suspected to have played a role in delays before successful completion of Dell's acquisition of EMC and Marriott International's acquisition of Starwood Hotels and Resorts, both of which were transactions involving U.S. companies.

[113] Yonnex Li, "Comment: Qualcomm's Arriver bid draws focus on geopolitics more than antitrust in China," MLEX (Oct. 8, 2021) (explaining that a Swedish company, Veoneer, cancelled a previously agreed upon deal with a Canadian company in order to be acquired by Qualcomm for an additional $700 million, and concluding that "Veoneer's choice shows that it is willing to take a greater regulatory risk for a higher offer, considering Qualcomm's inability to obtain Chinese antitrust approval for the NXP" deal in 2018).

what they had been led to believe was to be a celebration of the AML's five-year anniversary.[114]

More recently, with changed leadership and the integration of NDRC's Price Supervision/Inspection Bureau and MOFCOM's Anti-Monopoly Bureau into SAMR and now SAMR's new and enlarged National Anti-Monopoly Bureau – and the gradual professionalization of AML enforcement in China overall – overt discrimination against foreign companies in abuse of dominance investigations has abated. However, SAMR has initiated several abuse of dominance investigations targeting foreign companies in industries that China considers strategic – contributing to concerns that industrial policy likely continues to motivate AML enforcement in this regard.[115]

C. IP-related competition law rules

In September 2020, SAMR released the Anti-Monopoly Guidelines in the Field of Intellectual Property Rights ("IP Guidelines"). The IP Guidelines contain several provisions that appear to press the transfer of technology from foreign companies to Chinese companies and/or to lower the value of foreign IP licenses.

For example, the IP Guidelines establish a six-factor framework by which SAMR can determine whether a company's refusal to license to Chinese companies may constitute abuse of a dominant market position. The factors to be considered by SAMR include the impact that a refusal to license could have on competition and innovation in the market, whether the licensor has proposed a reasonable offer to the party seeking a license, and whether the license of the IPR in question is essential for entry into the relevant market. Such factors focusing on the impact on Chinese companies run contrary to how U.S. and European antitrust agencies traditionally

---

[114] In addition, between 2014 and 2015, SAMR's predecessor agencies conducted a series of investigations targeting bundling and interoperability of Microsoft's Windows and Office products; Chrysler, Audi, BMW and Mercedes for alleged price fixing; U.S. chipmaker Qualcomm; and a group of infant milk powder suppliers including U.S.-based Mead Johnson. Several of these companies were fined tens of millions of dollars, and Qualcomm was assessed a then-record USD $975 million fine. Chinese antitrust regulators reportedly conducted early-morning raids on corporate offices and brought in representatives of these firms into meeting, urging them "to confess to any antitrust violations." *See* Michael Martina & Kazunori Takada, "Rattled by investigations, foreign firms in China beef up compliance," REUTERS (Sept. 2, 2013).

[115] In 2019, SAMR or its provincial counterparts issued large financial penalties against foreign companies in three investigations: a $3.6 million fine against the Chinese subsidiary of U.S. chemicals producer Eastman for abuse of dominance in the market to secure exclusive dealing rights with clients and distributors, a $12.5 million fine against Toyota for resale price maintenance (RPM), and a $23.5 million fine against Ford Motor's joint venture in China also for RPM. *See* "Shanghai Administration for Market Regulation fines Eastman unit for abuse of dominance," PARR (Apr. 29, 2019). Other jurisdictions have held that vertical agreements should be analyzed under a rule of reason rather than deemed to be *per se* illegal. *See, e.g.*, Leegin Creative Leather Products, Inc. v. PSKS, Inc., 551 U.S. 877 (2007).

analyze the assertion of intellectual property rights in the antitrust context. The recent issuance of the IP Guidelines could foretell a more aggressive stance, with antitrust regulators determining that IP rights-holding companies have engaged in anticompetitive behavior merely for negotiating assertively in licensing negotiations with Chinese parties or refusing to license IP for otherwise legitimate reasons (e.g., fear of misappropriation).

In addition, antitrust principles are increasingly being used in Chinese courts to undermine foreign companies' IP rights. In June 2021, an intermediate court in Zhejiang Province just south of Shanghai resolved a longstanding dispute between the Japanese steel and metals manufacturer Hitachi Metals and Chinese rare earths materials companies, by issuing the first court decision in China that a company's patents were de-facto essential. Invoking the "essential facilities" doctrine, the Chinese court held that Hitachi Metals' refusal to license these "essential" patents to some Chinese companies constituted an abuse of its market dominant position.[116] Although this case was filed in 2016, well before the IP Guidelines were issued, the case is expected to be appealed to the Intellectual Property Court of the Supreme People's Court (SPC IPC), a recently-created, nationwide appellate body with specific focus on intellectual property and antitrust issues. The new IP Guidelines may indicate that a decision from the SPC IPC that further weakens foreign companies' IP protections is forthcoming.

III. Broader Policy and Regulatory Initiatives that Promote Chinese Technology Companies and Disadvantage Their Foreign Competitors

Beyond the AML, China uses a wide range of legal and regulatory tools to advance its overarching techno-nationalist agenda. Select examples are listed below. Additional measures are discussed in various reports issued by the Office of the U.S. Trade Representative.[117]

Massive subsidies to Chinese industry. Targeted subsidies for key industries have long been a part of China's strategy to grow its economy, but in recent years China's subsidy programs have become more sophisticated and intertwined in such broader initiatives as the Made in China 2025 campaign and the Belt and Road

[116] Anjie Law Firm, "Essential or Not? The Perils of Mandatory Licensing for Non-SEPs in China: Case Comments on Four Local Rare Earth Magnet Companies v. Hitachi Metals," CHINA LAW VISION (Sept. 2, 2021).

[117] *See, e.g.*, Office of the U.S. Trade Representative, "2021 National Trade Estimate Report on Foreign Trade Barriers" (Mar. 2021) at 95-130; Office of the U.S. Trade Representative, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974" (Mar. 22, 2018).

Initiative ("BRI"), President Xi Jinping's signature foreign policy initiative.[118] China has launched massive subsidy programs to promote strategic industries in particular. For example, China has established a network of private equity-like funds to promote China's industrial policy objectives in the semiconductor and integrated circuit sector, with hundreds of billions of dollars in funding. In addition, in 2020, China's Ministry of Industry and Information Technology announced plans to contribute about $1.4 trillion in investment over the next five years into AI, data centers, mobile communications, and other projects.[119] China also gives a wide range of subsidies to Chinese ICT firms engaged in overseas development projects in connection with the BRI, such as building data storage facilities and network infrastructure.[120]

Excluding U.S. technology firms from China's market. For years, the Chinese government has placed restrictions on the ability of U.S. technology firms to operate within China's market. China's vast internet censorship regime has made it impossible for companies such as Google or Facebook to provide their flagship products to users located in mainland China. Microsoft's LinkedIn and Yahoo also recently exited China – marking the end of U.S. social media and internet search engines' presence in China – at least in part a reflection of the increasing difficulty of compliance with the new data protection laws discussed below.[121]

Other U.S. technology companies are cut off from the Chinese market by the Chinese government's narrowing but still broad restrictions on inbound investments, including a "negative list" of sectors in which foreign investment is prohibited or restricted, as well as rules that require information and communications technology infrastructure to be "secure and controllable" or "secure and reliable" – criteria that foreign companies generally cannot meet. Furthermore, the Chinese government has indicated its intent to continue developing policy in this direction. Since 2020, China's leadership has stressed the concept of a "dual circulation" economic model,

---

[118] The BRI's roots trace back to other regional initiatives launched by President Hu Jintao. *See, e.g.*, Rush Doshi "Hu's to blame for China's foreign assertiveness," BROOKINGS (Jan. 22, 2019); Kawashima Shin, "The Belt and Road Initiative: Responding to Beijing's Ambitious Endeavor," NIPPON (June 13, 2018).

[119] *See* Liza Lin, "China's Trillion-Dollar Campaign Fuels a Tech Race With the U.S.," THE WALL STREET JOURNAL (June 11, 2020).

[120] "China's Belt and Road: Implications for the United States," Independent Task Force Report No. 79, COUNCIL ON FOREIGN RELATIONS (Mar. 2021) at 23-24, 70 (hereinafter "CFR Report").

[121] Liza Lin, "Yahoo Pulls Out of China, Ending Tumultuous Two-Decade Relationship," THE WALL STREET JOURNAL (Nov. 2, 2021); Aaron Tilley & Liza Lin, "LinkedIn Social Network Is Leaving China, but Microsoft Remains," THE WALL STREET JOURNAL (Oct. 15, 2021). LinkedIn and Microsoft's Bing search engine along with hundreds of locally-developed apps were notified by the Cyberspace Administration of China that they had excessively collected and illegally accessed users' personal information. *See* "Announcement of the illegal collection and use of personal information by 105 apps including Douyin," Cyberspace Administration of China (May 21, 2021); *see also* Zen Soo, "China authorities name 105 apps for improper data practices," ASSOCIATED PRESS (May 21, 2021).

which represents an ambition for China "to become a fully integrated market with no need for help from the rest of the world, though still benefiting from export markets."[122]

Complex and burdensome data security regime. China has adopted a series of data security laws and regulations that have made it increasingly difficult for U.S. and other foreign companies to operate in China. The Cybersecurity Law (effective June 1, 2017), the Data Security Law (effective September 2021), and the Personal Information Protection Law (effective November 2021) together impose broad data localization requirements – severely restricting cross-border transfers of information that are routine in the ordinary course of business and are fundamental to business activity. The Chinese government's intent to comprehensively enforce these restrictions was most recently made clear in the *Opinions on Promoting the Healthy and Sustainable Development of the Platform Economy* released in January 2022, which calls for strengthening a "graded classification + negative list" supervision system to restrict cross-border data flows.[123] Not only must foreign companies operating in China store business and personal data there, but they must also hand over data to Chinese government authorities upon request, without a warrant, to facilitate law enforcement activity and judicial proceedings. Companies that defy such laws face heavy monetary fines. In August 2021, China released a draft of a sweeping, first-of-its kind regulation on the use of algorithmic recommendations.[124] In October 2021, the Cyberspace Administration of China announced a three-year campaign that entails registration of algorithms and the Chinese government's deployment of a technical team to evaluate risks posed by tech company algorithms.[125] The Sixth Plenum Report that emerged from the critical November 2021 Party meetings to chart the course for President Xi's next term indicates that data security will continue to be an area of focus for the Chinese government. This report underscored that the CCP and the Chinese government will strengthen the protection of data involving national interests, trade secrets and personal privacy, and seeks to "actively participate" in

---

[122] *See* Alicia García Herrero, "What is Behind China's Dual Circulation Strategy," CHINA LEADERSHIP MONITOR (Sept. 1, 2021) ("dual circulation is part of China's masterplan to become self-reliant in terms of resources and technology but also in terms of demand through its huge market as well as through third markets available through the BRI."); *see also* "The Fourteenth Five-Year Plan for the National Economic and Social Development of the People's Republic of China and the Outline of the Long-term Goals for 2035," The Central People's Government of the People's Republic of China (Mar. 13, 2021).
[123] *See* "The Opinions of the National Development and Reform Commission and Relevant Departments on Promoting the Healthy and Sustainable Development of the Platform Economy," NDRC.gov.cn (January 19, 2022) [Guojia fazhan gaige wei deng bumen guanyu tuidong pingtai jingji guifan jiankang chixu fazhan de ruogan yijian].
[124] Internet Information Service Algorithmic Recommendation Management Provisions [Hulianwang xinxi fuwu suanfa tuijian guanli guiding] (Opinion-Seeking Draft) Aug. 27, 2021.
[125] Stephanie Yang, "China Leaps Ahead in Effort to Rein in Algorithms," THE WALL STREET JOURNAL (Oct. 5, 2021).

shaping international rules around data security, including promoting the "secure and orderly flow of data across borders."[126]

Aggressive campaign to influence standardization. In recent years, China has steadily increased its role in various international standard-setting organizations that may influence the development of critical technologies such as 5G, AI, and the Internet of Things (IoT). This will enable products produced by Chinese companies to be designed and produced at scale and used worldwide as well as in China's large domestic market. By the same token, companies that do not use such standards may risk facing shrinking global markets.

China articulated its ambitions with respect to standard-setting in the Made in China 2025 industrial plan, as well as the October 2021 National Standardization Development Outline ("Outline") (which has apparently superseded the prior plan, known as China Standards 2035).[127] The Outline sets goals for China to set standards for the commercialization of cutting-edge technologies such as robotics, high-speed rail, big data, AI, renewable energy vehicles, and biotechnology. The CCP Central Committee (acting on behalf of the Politburo Standing Committee) and the State Council (the central administrative authority of the Chinese government) jointly released the Outline, indicating the importance of standard-setting to China's broader industrial policy.

In addition, the number of Chinese companies participating as voting members of the Third Generation Partnership Project (3GPP), the multi-stakeholder body responsible for setting 5G standards, has increased significantly in recent years, with 110 Chinese companies now participating as voting members as of January 2020 (compared to 53 U.S. voting companies).[128] Overall, between 2010 and 2020, China has increased the number of its representatives in technical committees and subcommittees by 73%, reaching approximate parity with Japanese representatives while approaching the number of German and U.S. representatives.[129] On a parallel track, China has pursued bilateral "mutual recognition" with a number of nations on standards already used by China while using BRI to further promote adoption of its preferred technical standards.[130]

---

[126] *See* Resolution of the CCP Central Committee on the Major Achievements and Historical Experience of the Party Over the Past Century, Part V, Article XVIII, Sections 1 and 4.
[127] National Standardization Development Outline, Central Committee of the Communist Party of China and the State Council (Oct. 10, 2021).
[128] "China in International Standard Setting: USCBC Recommendations for Constructive Participation," THE U.S.-CHINA BUSINESS COUNCIL (Feb. 2020), at 3.
[129] *See id.*
[130] John Seaman, "China and the New Geopolitics of Technical Standardization," FRENCH INSTITUTE OF INTERNATIONAL RELATIONS (Jan. 2020).

Actions Taken by China's Judiciary that Weaken IP. In recent months, China's courts taken significant steps that weaken IP rights for foreign rights holders. For example, they have begun to grant "anti-suit injunctions" that prevent foreign IP holders from enforcing their IP rights against Chinese companies in foreign jurisdictions.[131] The injunctions are granted in *ex parte* proceedings – meaning that foreign companies have no opportunity to participate – and in at least one case involving Huawei the injunction was granted within 48 hours of the application.

Anti-suit injunctions give Chinese companies leverage to invalidate patents and strong-arm foreign companies operating in China to sign licensing agreements favorable to Chinese companies.[132] The use of anti-suit injunctions to promote China's industrial policy goals is congruent with the Chinese judicial system's limited independence from the CCP. In fact, China's laws mandate that its courts prioritize the Party's goals, China's laws and other regulations over foreign court judgments, and in practice Chinese courts are often influenced by large domestic companies, local governments, and regulators.

In addition, in August 2021, the Supreme People's Court (SPC) issued a landmark ruling in *Oppo v. Sharp*, pertaining to standard essential patent (SEP) licensing. In particular, the SPC ruled that Chinese courts could set the terms of a global FRAND license, including licensing fees, under certain circumstances – even over the objections of one of the parties (in this case, the foreign licensor).[133] This troubling ruling shows that Chinese licensees have the option to resort to litigation in Chinese courts to obtain global SEP licensing terms more favorable than those that they are able to obtain through negotiations with foreign licensors – eroding the value of the IP at issue.

A. The "Tech-Crackdown" in China

Since late 2020, the Chinese government has taken a series of regulatory actions to restructure significant sectors of its economy, including levying antitrust fines and denying merger approvals to China's leading technology companies. Although the actions taken against Didi Chuxing, Alibaba, Tencent, and Meituan were the most notable for U.S. markets and media outlets, these actions against China's

[131] In 2020, several Chinese courts have granted global anti-suit injunctions upon applications from Chinese tech companies Huawei, Xiaomi, and BBK Electronics. In the case involving Xiaomi, a Delaware-based company sought to bring a patent infringement case against Xiaomi. But before that suit was filed, a court in Wuhan issued an anti-suit injunction that barred the U.S. company from suing Xiaomi, and further warned that the U.S. company would face weekly fines of $1 million if it violated that injunction.

[132] Josh Zumbrun, "China Wields New Legal Weapon to Fight Claims of Intellectual Property Theft," THE WALL STREET JOURNAL (Sept. 26, 2021).

[133] China's Supreme People's Court Affirms Right to Set Royalty Rights Worldwide in OPPO/Sharp Standard Essential Patent Case, National Law Review (Dec. 10, 2021).

leading tech companies are part of a broader reorientation of China's economy. Observers have identified several possible motivations for the Chinese government's decision to reorder its economic system, such as an effort to address lagging social mobility and a growing wealth gap,[134] or a desire to emphasize the prominence of President Xi and the Party in advance of key meetings that took place in November 2021.[135]

While the Chinese government's precise motivations for launching this campaign to transform broad sectors of the Chinese economy are unclear, there is no indication that China is abandoning its longstanding policy objective of bolstering the competitiveness of its domestic companies and SOEs vis-à-vis U.S. companies. None of the draft guidelines or recently implemented data, cybersecurity, or privacy laws include plans to break up China's largest and most successful tech companies or to restrict the ability of those companies to merge with or acquire other tech companies.[136] To the contrary, numerous policy documents show that China expects its leading technology companies to continue leveraging their scale and capabilities to attain dominance in strategically important sectors, as opposed to less strategic sectors like electronic games. For example, China's 14th Five-Year Economic and Social Development Plan (released in March 2021) calls for China to build industrial scale advantages, to consolidate its first-mover advantages, and increase the competitiveness of its entire production chain in high-speed rail, new energy, shipping, and other strategic fields.[137] Similarly, the *Opinions on Promoting the Healthy and Sustainable Development of the Platform Economy* ("Opinions") explicitly direct regulators to support "powerful leading enterprises" in promoting "key software technology research" related to "the underlying architecture of the industrial Internet" and "blockchain underlying technology."[138] The Opinions also call for regulators to encourage platform enterprises to increase R&D investment and accelerate "technological research and development breakthroughs" in critical technologies including AI, cloud computing, blockchain, operating systems, and processors. Such

[134] Stella Yifan Xie, "What's Driving Xi Jinping's Economic Revamp? China's Social Mobility Has Stalled," THE WALL STREET JOURNAL (Nov. 14, 2021).
[135] Charles Mok, "More than a Tech Crackdown, It's Farewell to China's Economic Reform," FRIEDRICH NAUMANN FOUNDATION FOR FREEDOM (Aug. 20, 2021);
[136] *See, e.g.*, Guidelines for Implementing Main Responsibilities of Internet Platforms (Draft for Comments), State Administration for Market Regulation (Oct. 29, 2021). [Hulianwang pingtai luoshi zhuti zeren zhinian]
[137] Outline of the People's Republic of China, 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, XINHUA (Mar. 12, 2021) [Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisi ge wu nian guihua he 2035 nian yuanjing mubiao gangyao]
[138] *See* "The Opinions of the National Development and Reform Commission and Relevant Departments on Promoting the Healthy and Sustainable Development of the Platform Economy," NDRC.gov.cn (January 19, 2022) [Guojia fazhan gaige wei deng bumen guanyu tuidong pingtai jingji guifan jiankang chixu fazhan de ruogan yijian].

goals would be unattainable if China sought to break up its tech giants and restrict their M&A activity.

Instead, the regulatory curbs on China's tech industry may have the impact of reorienting capital and talent away from consumer-oriented, social media and digital-economy technology companies to strategic technology industries such as semiconductors, electronics, technology, batteries, biotechnology, and telecommunications infrastructure. Tencent, for example, which has been impacted by China's imposition of weekly video game time limitations for children, recently announced that it has designed semiconductors to be used in AI computing and video processing, technologies that are prioritized by the Chinese government.[139] Similarly, Baidu has recently unveiled its second-generation AI chip and progress on its autonomous driving technology, while Alibaba has publicly announced progress made on its own server chip.[140]

Another strategy for Chinese tech giants to adapt to domestic regulatory scrutiny has been to focus on growth abroad—a trend actively encouraged by a wide array of regulatory guidance. For instance, the Opinions direct authorities to support platform companies to "promote digital products and services to 'go global,' enhance their international development capabilities, and enhance their international competitiveness."[141] This type of direct guidance has motivated Chinese tech giants that have come under regulatory scrutiny to curry government favor by expanding their investments and operations abroad. For example, in the first six months of 2021, Tencent completed 34 international investments, compared to just 4 and 3 international deals over the same periods in 2020 and 2019, respectively.[142] These decisions by China's technology giants to either pivot to strategic technology sectors or to acquire companies abroad are strong indications that the tech industry will likely emerge from China's current campaign more aligned with the Chinese government's broader industrial policy goals and prepared to serve the Chinese government's interests through their activity abroad.

---

[139] Yifan Wang, "China's Tougher Regulation Is the New Normal, Tencent President Says," THE WALL STREET JOURNAL (Nov. 10, 2021).

[140] Arjun Kharpal & Evelyn Cheng, "China's Baidu launches second chip and a 'robocar' as it sets up future in AI and autonomous driving," CNBC (Aug. 18, 2021); Coco Liu & Debby Wu, "Alibaba Just Unveiled One of China's Most Advanced Chips," TIME (Oct. 18, 2021).

[141] *See* "The Opinions of the National Development and Reform Commission and Relevant Departments on Promoting the Healthy and Sustainable Development of the Platform Economy," NDRC.gov.cn (January 19, 2022) [Guojia fazhan gaige wei deng bumen guanyu tuidong pingtai jingji guifan jiankang chixu fazhan de ruogan yijian].

[142] Mercedes Ruehl & Primrose Riordan, "Tencent boosts global investments as Beijing cracks down on gaming," FINANCIAL TIMES (Sept. 1, 2021).

IV. The EU Is Pursuing a Digital Sovereignty Agenda to Support the Emergence and Growth of EU Technology Companies While Constraining U.S. Competitors

The EU is pursuing a "digital sovereignty" agenda as a means to promote European leadership and strategic autonomy in the digital field.[143] The agenda is intended in part to reduce what is perceived as overreliance on U.S. technology companies. In many ways, the EU's digital sovereignty agenda takes a page from China's industrial policy playbook, using subsidies and idiosyncratic, often discriminatory regulation to clear space in the market for domestic competitors to grow and thrive, while limiting competition from foreign rivals.

Among the most significant initiatives in this context are the Digital Markets Act, a legislative proposal which, like the U.S. antitrust legislation discussed above, targets successful U.S. technology companies – as well as the Gaia-X state-led cloud project and the EU Data Act.

A. The Digital Markets Act

In December 2020, the European Commission ("EC") issued a legislative proposal, the Digital Markets Act ("DMA"), which is intended to regulate business practices of large online platforms, or so-called "gatekeepers." The DMA is structured to impose significant new obligations on large U.S. technology companies, while leaving EU and other foreign companies unaffected.[144]

The EU has been concerned about the perceived market power of U.S. digital platforms for many years. Historically, it has used competition law to address its concerns, initiating a series of high-profile investigations against such companies as Amazon, Apple, Facebook, Google, Intel and Microsoft. However, EU policymakers have now concluded that its existing competition laws are inadequate for this purpose, apparently because investigations take too long and there are "high legal thresholds to prove abuse."[145] In a break with current competition law norms, the DMA would eliminate these impediments by creating a new regulatory framework for "gatekeepers" that would impose restrictions on platforms on an *ex ante* basis – *i.e.*, without any anticompetitive conduct having actually taken place and eliminating the need to prove consumer harm. The DMA is similar in this respect and others to the

[143] Tambiama André Madiega, *Digital sovereignty for Europe*, European Parliament Research Service (EPRS) Ideas Paper - Towards a more resilient EU (July 2, 2020) at 1.
[144] Cristina Caffarra & Fiona Scott Morton, *How Will the Digital Markets Act Regulate Big Tech?*, Contexte Numérique (Jan. 11, 2021).
[145] Digital Markets Act Impact Assessment support study (Dec. 2020) ("Impact Assessment support study") at 17.

U.S. legislation discussed above, and if implemented, will set a troubling regulatory template for other countries.

i. Scope of application: the DMA targets U.S. companies

As indicated in the EC's preparatory work, the DMA focuses primarily on large foreign platforms. For example, in its Inception Impact Assessment setting a roadmap for future legislation on *ex ante* regulatory instruments in the digital sector, the EC identifies "a small number of large online platforms" as the DMA's targets.[146] In the subsequent Impact Assessment Report, which accompanies the DMA, the EC discusses, among other things, the supposed "unfair practices" that the new rules are intended to address – citing as examples various types of conduct by U.S. companies such as Amazon, Apple, Facebook, Google, and Microsoft.[147] By contrast, the only example involving a non-U.S. company refers to Naver, a Korean firm.[148] No European companies are mentioned.

Based on this approach, the EC devised criteria for the definition of gatekeepers which, not coincidentally, cover U.S. companies and exclude European companies offering similar services. In particular, under the current draft of the DMA, a company providing a core platform service will be regulated as a gatekeeper under the DMA when the company meets the following metrics: (a) annual turnover in the EEA at or above EUR 8 billion in the past three years or market value of at least EUR 80 billion in the last year and core platform service provision in at least three EU member states; and (b) provision of one or more core platform services, each of which has more than 45 million monthly end-users in the EEA and more than 10,000 yearly business users in the EEA in each of the last two years.[149]

Companies that meet these quantitative thresholds are subject to a rebuttable presumption that they are gatekeepers. Once officially categorized as gatekeepers under the DMA, companies must comply with the DMA's obligations (discussed below).[150] For each entity that meets the gatekeeper thresholds, the EC will designate

[146] DMA Inception Impact Assessment: Ex ante regulatory instrument for large online platforms with significant network effects acting as gatekeepers in the European Union's internal market (June 2, 2020) at 2 ("a small number of large online platforms increasingly determines the parameters for future innovations, consumer choice and competition. Consequently, Europe's estimated 10,000 online platforms are potentially hampered in scaling broadly as they are increasingly faced with incontestable online platform ecosystems.").
[147] *Id.* at 53-60.
[148] *Id.* at 57.
[149] DMA, Art. 3.
[150] *Id*; see also DMA, Art. 5 and 6.

the specific core platforms provided by the gatekeeper that fall within the scope of the DMA.[151]

Based on the legislation as currently structured, it appears that companies that meet these quantitative thresholds will have an opportunity to rebut the presumption only by "compelling arguments" which refer to structural market characteristics (e.g., no entry barriers or lock-in/dependence of business or end users). By contrast, it is not possible for them to rebut the presumption by reference to procompetitive efficiencies their practices may generate.[152]

In practice, the DMA's high quantitative thresholds will likely be met by several U.S. companies, including Amazon, Apple, Facebook, Google, and Microsoft. By contrast, at present, no European companies that offer like services are likely to meet these thresholds. This has been repeatedly acknowledged, among others, by members of the European Parliament commenting on the DMA. For instance, Czech Member of European Parliament Dita Charanzová wrote that "we must state the truth: these proposals target US companies."[153] Meanwhile, Andreas Schwab, s a German Member of European Parliament and the European Parliament's rapporteur for the DMA, has repeatedly called for the need to limit the scope of the DMA to non-European firms. In May 2021, he stated, "Let's focus first on the biggest problems, on the biggest bottlenecks. Let's go down the line – one, two, three, four, five – and maybe six with Alibaba. But let's not start with number seven to include a European gatekeeper just to please [U.S. president Joe] Biden."[154]

In this context, it should be noted that the draft report on the DMA, issued by the Internal Market and Consumer Protection ("IMCO") committee of the European Parliament in June 2021 and presented by Mr. Schwab ("the Schwab Report"), suggested that the quantitative thresholds provided in the EC's initial proposal be raised to an annual EEA turnover at or above EUR 10 billion (instead of the initial EUR 6.5 billion), a market value of at least EUR 100 billion (instead of the initial EUR 65 billion) and the provision of two or more core platform services (instead of just one, as was provided initially). The aim of these proposed amendments is to "clearly targe[t] [...] those platforms that play an unquestionable role as gatekeepers due to their size

[151] DMA, Art. 3. The EC has the authority to designate additional digital services as core platform services that could fall within the scope of the DMA.
[152] *Id*.
[153] Dita Charanzová, *Turning Europe's internet into a 'walled garden' is the wrong path to take*, Financial Times (Feb. 17, 2021).
[154] Javier Espinoza, *EU should focus on top 5 tech companies, says leading MEP*, Financial Times (May 31, 2021).

and their impact on the internal market"[155] – in other words, to ensure that the DMA is targeted as squarely as possible at U.S. technology companies. These amendments were already approved, in part, by the European Parliament's IMCO committee on November 23, 2021.

ii. Requirements for companies deemed "gatekeepers" under the DMA

Articles 5 and 6 of the DMA contain two sets of key obligations that would apply no later than four months after identification as a gatekeeper with respect to a designated core platform service. Under these obligations, gatekeepers will have to, among other things:

- Allow business users of the platform to offer the same products on other platforms subject to differing conditions;
- Disclose prices paid by advertising/publisher customers, and amounts paid to publishers, for publishing an ad or providing ad services;
- Refrain from using data that is not publicly available (*i.e.*, because it is generated through activity by business users or their end customers on the core platform) in order to compete with business users;
- Refrain from combining personal data sourced from a core platform service with personal data from other services (whether core platform services or not) provided by the "gatekeeper", or with third-party services. Gatekeepers may only combine such data if the end user has consented to this in the sense of the EU General Data Protection Regulation 2016/679 ("GDPR").
- Rank third-party products and services on a fair and non-discriminatory basis and refrain from treating the gatekeeper's own products and services more favorably;
- Allow third-party providers of online search engines (or entities contracted by these providers) access on fair, reasonable and non-discriminatory (FRAND) terms to ranking, query, click, and view data generated by searches of end users using the online search engine of the gatekeeper;
- Allow third-party apps/app stores to be installed and used interoperably with the core platform's operating system, even if these third-party apps

[155] Draft Report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 - C9-0419/2020 - 2020/0374(COD)), European Parliament, Committee on the Internal Market and Consumer Protection, at 32-33.

are accessed without use of the core platform services, subject to protecting the technical integrity of the platform;

- Allow business users (including competitors) continuous and real-time access to user data and data generated from users' interactions with their products on the gatekeeper's platform; and
- Provide third-party free of charge access to and interoperability with all hardware and software features that are accessed or controlled via the gatekeeper's core platform service operating system.[156]

Several of these provisions resemble those in the U.S. legislation discussed above, including provisions related to access to user data, portability of user data, interoperability, and non-discrimination with respect to the products, services, and lines of business of other companies. In fact, certain provisions – including the requirements to disclose data related to online searches – actively undermine the protection of trade secrets and intellectual property rights that Europe has long championed. The U.S. Government highlighted these concerns in a document circulated to the EC, EU member states, and involved companies.[157] These provisions of the DMA would force U.S. companies to share confidential data and proprietary information not only with their European competitors, but also with state-owned and state-backed firms from non-market economies like China.

Rather than tailored measures to prevent specific perceived market failures, the DMA follows an inflexible, "one-size-fits-all" approach, based on size thresholds. As noted above, the obligations in question are imposed on "gatekeepers" without a need to prove anticompetitive conduct or consumer harm. Nor is it possible for companies to argue, e.g., that their practices have no competitive impact or are in fact procompetitive because they generate efficiencies that benefit users.[158]

A gatekeeper can incur fines of no less than 4% and not exceeding 20% of its worldwide turnover in the preceding financial year for breach of these obligations. The EC may also impose behavioral or structural remedies if a gatekeeper systematically breaches the obligations (two or more non-compliance or fining decisions within ten years) and further strengthens its gatekeeper position.[159]

B. The Gaia-X Project and the EU Data Act

[156] The EC has the authority to add additional obligations to these lists where it has identified practices that limit core platform contestability or are unfair in the same way as those already listed in the DMA.
[157] Foo Yun Chee, *U.S. warns against IP, trade secret risks in draft EU tech rules - paper*, Reuters (Nov. 10, 2021).
[158] DMA, Art. 3; see also Art. 5 and 6.
[159] DMA, Art. 16 and 26.

Gaia-X is a subsidy-fueled initiative for the development of a state-led federation of data infrastructure and service providers for Europe. Gaia-X echoes an earlier EU industrial project: Airbus. Decades ago, the EU used subsidies to create Airbus as a competitor to the United States in aerospace – and the World Trade Organization later found the associated subsidies to be inconsistent with global trading rules. Now the EU is seeking to do the same in the cloud space with Gaia-X.

Initially launched in 2019 as a joint Franco-German project, Gaia-X is now a key building block of the European Digital Strategy. Its aim is to establish an interoperable data exchange under the protection of EU law, with the goal of reducing the EU's reliance on non-European cloud providers, specifically large U.S. technology companies. For example, the Gaia-X website states: "these [non-European] providers are able to rapidly scale their infrastructure, and hold significant market power and large amounts of capital. At the same time, we are seeing growing international tensions and trade conflicts across the globe. Europe needs to ensure that it can establish and maintain digital sovereignty permanently."

In that context, there are proposals for a labeling system, which would indicate the level of security provided by a cloud service. Companies participating in Gaia-X would therefore "be able to offer customers a label ensuring that their data is being stored and processed in Europe."[160] Earlier this year, Germany's Federal Ministry for Economic Affairs and Energy announced plans to award approximately EUR 122 million in a first round of funding to demonstrate the viability and usability of Gaia-X.[161]

In addition, since the autumn of 2020, the EC, together with eleven EU member states, has been working on a new Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services ("IPCEI-CIS"). This is presented as another "important foundation for Europe's digital sovereignty,"[162] after Gaia-X. Essentially, this is a new funding scheme that will allow EU member states to directly subsidize this sector, with a more flexible – and in effect, more limited – applicability of traditional EU state aid limitations.

The EU is also developing a legislative proposal for a Data Act, set to be published in early 2022. This proposal is intended to foster business-to-government data sharing for the public interest, support business-to-business data sharing, and

---

[160] Clothilde Goujard, *Gaia-X draft rules enshrine EU data localization as security option*, PoliticoPro (Nov. 8, 2021).
[161] Federal Network Agency, *Gaia-X: winning consortia in funding competition* (June 30, 2021).
[162] Federal Ministry for Economic Affairs and Energy, *Cloud IPCEI entering next phase as call for expressions of interest is launched in Germany and preparations for European matchmaking process get underway*
Introduction (July 9, 2021).

evaluate the current EU IPR framework with a view to further enhancing data access and use. A review of the current rules on the legal protection of databases is also part of this initiative.

Should the Data Act mandate data sharing between businesses or between businesses and governments, it would introduce even more risks for U.S. technology companies operating in Europe. Concerningly, the initial drafts of the Data Act also call for increased data localization for non-personal data – expanding far beyond the existing limitations on the transfer of personal data outside the EU. Although these initiatives are still in progress, they are important stepping stones in the EU's quest for enhanced "digital sovereignty."