CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

JANUARY 2025

Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology

Peter E. Harrell

Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology

Peter E. Harrell

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

On January 20, 2025, the first day of his second term, President Donald Trump sought to delay enforcement of a 2024 law that banned distribution of the popular Chinese-owned social media app TikTok. The intent of this delay was for his administration to work out a deal by which TikTok's Chinese parent, ByteDance, could divest the app. Regardless of the ultimate resolution of the TikTok case, restrictions on Chinese communications technologies, software, and internet-connected devices are becoming a major pillar of U.S. economic and technology policy toward Beijing, alongside tariffs and export controls. Over just the past twelve months, the United States cited potential electronic espionage as the basis for restricting the use of new Chinese cargo terminal cranes at U.S. ports, passed legislation and issued a new executive order limiting certain data transfers to China, imposed draft "Know Your Customer" (KYC) requirements on U.S. cloud services providers, published a draft rule to ban Chinese autonomous cars being sold or used on American roads, and launched a process to restrict the use of Chinese-made commercial and hobbyist drones—by far the world's most popular—in the United States. Indeed, while public attention in January focused on Trump's actions toward TikTok, a trade-related executive order that Trump signed his first day in office appeared to tee up an expansion of these sorts of restrictions on Chinese technologies.

Over the past decade, the United States quietly has built an increasingly extensive set of regulatory tools to regulate U.S. data flows to China and the operation of Chinese software and connected technologies in the United States. Although individual actions generally are tailored to address a specific risk, the growing sweep of regulatory authorities has the potential to dramatically change America's economic relationship with China, restricting

not only a growing array of internet-connected devices and consumer products made in China but also products made by Chinese companies in third countries. Beijing, meanwhile, is intensifying its mirror-image campaign against products made by U.S. firms, with the Chinese government imposing new security restrictions on U.S. semiconductors, computers, and other connected tech.[1]

American officials' desire to limit data flows to China and to restrict Chinese software and connected tech in the United States is understandable: China is America's foremost strategic competitor, and China's access to data and control of software and connected technology in the United States provides Beijing with potential tools to conduct espionage; influence politics; and, in extreme cases, attack critical infrastructure, commercial, and government networks inside the United States. But the central role that data, software, and connected technology play in the modern economy means that in principle restrictions could impact even anodyne-seeming trade, either because it depends on data or because even devices like toasters and thermostats increasingly connect to the internet.

Moreover, the United States and China are hardly alone in being concerned about dependence on foreign technology. A growing number of European experts and government officials would like to see the continent reduce its dependence on both Chinese and U.S. technology as a way of increasing Europe's own strategic autonomy. Since the late 1990s, American officials generally have argued against foreign government policies that would restrict data flows or limit software or connected technologies, believing that an open internet ecosystem would advance both American values and the commercial interests of U.S. firms. If the United States is now embracing restrictions on its own tech relationship with China, American officials will need to articulate a new vision for global data flows, software, and connected devices that enable allies to address their legitimate security interests while preserving the moral, commercial, and economic benefits of the open internet.

The current U.S. regulatory regime is spread across numerous government agencies and derives from multiple legal authorities. This paper is intended to help policymakers, business, and other stakeholders develop a more strategic approach to addressing the risks of China's access to U.S. data and control of software and connected tech. It begins by describing the three major sets of risks that need to be addressed: espionage; influence campaigns; and attacks on commercial, government, and civilian networks. It then traces the history of the emerging regulatory regime and describes its multiple constituent elements. Finally, it offers a set of recommendations to policymakers as they build out this area of work over the next several years.

The Risks of Chinese Access to Data and Control of Software and Connected Technologies

Since the late 2000s, and particularly over the past decade, three major factors have driven rising U.S. government concern about Chinese access to U.S. data and Chinese control of software and connected technology in the United States.

The first factor is China's emergence as America's primary strategic rival. Trump's 2017 National Security Strategy stated that "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity."[2] Former president Joe Biden's 2022 National Security Strategy stated that "The People's Republic of China harbors the intention and, increasingly, the capacity to reshape the international order in favor of one that tilts the global playing field to its benefit."[3] A bipartisan consensus has emerged across both Congress and executive branch officials that China presents a security and economic challenge and that Washington needs to develop policies to reduce Beijing's ability to conduct espionage and to establish leverage over the United States.

The second trend has been the rise of Chinese companies across important global technologies. When China first emerged as an economic power following Deng Xiaoping's economic reforms and opening in the 1980s, Chinese companies principally manufactured low-tech, comparatively low-value consumer items. Even as Western tech companies began to shift their manufacturing to China in the late 1990s and early 2000s, China's technology manufacturing consisted largely of assembly for Western-designed and operated products. That state of affairs changed during the 2000s and 2010s as Chinese firms became technological powerhouses in their own right. By the 2010s, Huawei and ZTE held significant market positions in international telecommunications network infrastructure, and today companies such as Xiaomi hold substantial shares of global mobile handset markets. Automotive companies like BYD rank among the world's largest electric vehicle manufacturers. Chinese heavy industry firm ZPMC manufactured 80 percent of the cranes used at American cargo ports.[4] And during the COVID-19 pandemic, social media platform TikTok became one of America's most popular apps, used by more than 150 million Americans monthly.

The third trend driving U.S. government concerns is China's extensive cyber hacking, which first emerged as a significant issue in the late 2000s. China-linked hackers appeared to infiltrate the 2008 presidential campaigns of both Barack Obama and John McCain, and over the following years Beijing's hackers targeted an ever-expanding range of U.S. corporate and government networks.[5] U.S. government officials recently have expressed concern that Chinese hacking efforts are intended to give China the ability to disrupt computer

networks, infrastructure, and business in the United States, and Chinese objectives are no longer limited to espionage activities.[6] Although publicly reported cases of Chinese hacking generally have not relied on the cooperation of China's own international tech companies, China's extensive hacking efforts provide a basis for U.S. government concerns that China could exploit its companies in the future, particularly as the companies achieve greater scale in U.S. and global markets.

Against this backdrop, there are four broad categories of risk associated with China's access to U.S. data and Chinese company control of software and connected technologies:

1. espionage and data security risks;
2. influence campaigns;
3. potential cyber attacks on critical infrastructure and government operations; and
4. potential use of connected devices to mount physical attacks inside the United States.

Espionage and data security risks: The first major category of risk is China's ability to leverage data, software, and connected technologies for espionage purposes and to secure access to data for other purposes potentially harmful to U.S. interests. Trump administration officials, for example, cited the risk of espionage as a major rationale for restricting Huawei and other Chinese telecommunications network infrastructure companies from providing equipment for U.S. telecommunications networks. Government officials have cited espionage risks as a justification for restricting the use of Chinese-made security cameras in the United States and as a primary justification for the data security executive order that Biden signed in 2024.[7] Chinese autonomous cars driving on U.S. roads collect substantial, detailed information about their surroundings. Even Chinese-made subway or rail cars contain sophisticated sensors that could be used for espionage.[8] An app like TikTok collects data about its users, including their location data, that could be exploited for espionage purposes. China could use such data to train AI systems and review real-time or recorded access to the feeds of U.S. security cameras or other sensors to monitor people and goods entering and specific facilities. Beyond espionage, China could seek access to proprietary datasets, such as genetic datasets, for AI training purposes to try to obtain an edge in aspects of AI development.

Influence campaigns: The second major category of risk, which is particularly associated with Chinese control of social media apps and similar software, is the risk of covert influence over U.S. public opinion. China is an active practitioner of global influence operations: a study released in 2024, for example, found that China is increasing covert social media and publicity campaigns to influence U.S. elections.[9] The U.S. government has highlighted this risk in legal filings related to TikTok. For instance, in a July 2024 filing, it stated that China

could use TikTok's algorithm to "illicitly interfere with our political system and political discourse, including our elections."[10] Other, more targeted types of influence are also possible. A Chinese-controlled smart television, for example, could disfavor ads from companies that have been critical of China, while an American company that depended on Chinese software or devices for vital parts of its own corporate information technology (IT) infrastructure could be blackmailed into staying silent on political issues important to Chinese officials.

Potential cyber attacks on critical infrastructure and government networks: A third major category or risks that U.S. officials have identified is the risk that China could leverage its control of software and connected technologies to mount cyber attacks on U.S. government networks and/or critical infrastructure in the United States. U.S. government officials are increasingly concerned that China's hacking of critical infrastructure providers is designed to provide China with an ability to attack and disrupt networks in the United States and not simply to conduct espionage. For example, the U.S. government has warned critical infrastructure operators that recent Chinese cyber intrusions may give China the ability to disrupt U.S. critical infrastructure during a Sino-U.S. conflict,[11] echoing long-standing concerns expressed by cybersecurity experts.[12]

Potential use of connected devices to mount physical attacks in the United States: Finally, officials are concerned that China could use connected devices such as internet connected vehicles or drones to mount physical attacks in the United States. Former commerce secretary Gina Raimondo focused on this set of risks when announcing plans to restrict the sale of Chinese connected cars in September 2024, arguing that "in extreme situations, a foreign adversary could shut down or take control of all their vehicles operating in the United States, all at the same time, causing crashes (or) blocking roads."[13] While widespread attacks are unlikely outside of the context of military conflict, the government is concerned about the possibility of more targeted attacks during peacetime as well as the potential for attacks during military conflict.

U.S. officials recognize that Chinese companies provide only one vector for China to conduct espionage, influence U.S. opinion, and threaten cyberattacks. Indeed, a public compilation of major cybersecurity incidents since 2006 maintained by the Center for Strategic and International Studies (CSIS) does not appear to include a single incident that clearly involves Beijing relying on a major international Chinese tech company to enable its hacking.[14] (That said, not all details regarding every documented hack have been made public, so it is possible that these hacks may have involved Chinese tech companies.) Moreover, Chinese companies typically assert their independence from Beijing: TikTok's CEO, for example, testified to Congress in 2023 that TikTok's parent company ByteDance "is not an agent of China" and that TikTok had never and would never share U.S. user data with the Chinese government.[15] The Chinese government doubtless also is aware that relying on a major Chinese tech company to facilitate hacking would result in that company—and potentially other Chinese companies—being excluded from global markets in the future. Such considerations may make Beijing wary of actively using Chinese companies to facilitate hacking until their products and services are already deeply embedded in global networks and difficult to remove.

These issues aside, there are at least three reasons to assess that Chinese companies with direct access to U.S. data or control of software or connected technology create risks beyond the inherent risks posed by Chinese hacking of U.S. and other Western firms.

First, bulk data transfers to China or Chinese control of software or connected devices provide an opportunity for significant, low-cost data collection. Purchases of bulk data can allow China or another U.S. adversary to inexpensively procure sensitive information about millions of individuals and can provide information on their interpersonal relationships and connections. Chinese autonomous driving companies collect detailed location data and imagery via sensors mounted on their cars and reportedly have driven more than 1.8 million miles in the United States—a potentially significant source of data.[16] TikTok has 150 million American users and could turn over substantial information about its userbase to Beijing if Beijing legally compelled it to do so.

Second, Chinese companies are subject to a set of legal regimes that could compel them to cooperate with Chinese defense and intelligence services. The legislation includes a national security law that establishes a "whole of society" approach to China's national security, including defining broad obligations for Chinese citizens to "provid[e] convenient conditions or other kinds of assistance to national security work" and to "provid[e] the necessary support and assistance to national security bodies, public security bodies and relevant military bodies."[17] A 2017 cybersecurity law requires cooperation with government inspections of networks and could enable Chinese government access to stored data.[18] Cyber vulnerability regulations from 2021 require Chinese companies to report cyber vulnerabilities to the Chinese Ministry of Industry and Information Technology within forty-eight hours of discovering them—almost certainly before patching the vulnerabilities or disclosing them to customers. This legal requirement could give Chinese hackers an opportunity to exploit the vulnerability before it is patched.[19]

A separate 2017 National Intelligence Law obliges Chinese companies and citizens to "support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of," which appears to authorize the Chinese government to compel its companies to support intelligence gathering.[20] A 2021 Counter Espionage Law mandates that Chinese nationals cooperate with China's national security agencies, and a 2023 update to the law widens the scope of the law to cover "documents, data, materials or items related to national security and interests."[21] And the growing presence of Chinese Communist Party (CCP) cells active in Chinese businesses may provide more informal ways for the Chinese government to exploit data, software, and connected devices.[22]

The third factor driving U.S. government concerns with China's control of software and connected tech is the potential for software and/or regular firmware and software updates from China to create particularly significant risks. The global IT meltdown that cybersecurity firm CloudStrike caused in July 2024 when it distributed a botched software update to

customers around the world—an event that likely caused between $5 billion and $10 billion in damage—illustrates the potential for updates to cause widespread disruptions.[23] Although encryption and third-party storage could help mitigate many data security risks, the potential for malware intrusions is high when a company maintains ongoing control of software—particularly when such control is combined with China's legal ability to compel a Chinese company to cooperate with Chinese defense and national security objectives.

Chinese and Third-Country Parallels

Although this paper is focused on Washington's growing concern about Chinese companies with access to U.S. data and control of software and connected devices, Beijing is engaged in a parallel campaign against what it perceives as the risks of U.S. firms that have access to Chinese data and that provide software and connected technologies in China.[24]

China has a long history of excluding U.S. technology companies and products, particularly news media outlets and social media platforms such as Facebook and YouTube, over censorship concerns. In the wake of Edward Snowden's revelations regarding American cyber espionage in 2013, China began to promote a "secure and controllable" IT sector that gradually would wean itself off foreign IT companies.[25] Initially, China's efforts to reduce its use of Western IT proceeded slowly, but Beijing has intensified the campaign in recent years. In 2022, the Chinese government reportedly issued an order for state-owned companies in critical sectors, including finance and energy, to replace non-Chinese software on their networks by the end of 2027.[26] Press reports suggest that many Chinese agencies and enterprises are banning employees from bringing phones manufactured by Western companies into government office buildings.[27] China also has targeted U.S. chipmakers: in 2023, it restricted the use of Micron chips from some domestic critical infrastructure networks, and in 2024, it announced plans to phase out Intel and AMD chips from government computers.[28] China also has taken broader measures to address perceived data security risks, notably far-reaching national data security laws that limit the flow of Chinese data internationally. And for U.S. tech companies that remain in China, Beijing increasingly is signaling that they will have to comply with measures to mitigate risk. In mid-2024, China gave U.S. car company Tesla permission to begin testing high-end autonomous driving features, which rely on precision imaging and sensors and large volumes of data, only after Tesla entered into a partnership with Chinese tech firm Baidu to help manage the data and mapping technology.[29] Tesla also recently passed a Chinese government data security audit that has allowed Tesla automobiles to be included on Chinese government procurement lists.

A number of other countries also have begun to take steps to reduce what they perceive as the risks associated with their reliance on both U.S. and Chinese tech companies. For example, in 2023 the European Union considered restrictions on the foreign ownership of companies providing certain cloud services in Europe, though in mid-2024 it dropped

proposed ownership restrictions in favor of data labeling and localization requirements.[30] Absent diplomatic work by Washington to reassure allies about the trustworthiness of U.S. firms, and the development of principles to differentiate the risks associated with U.S. technology from the risks of Chinese technology, this trend is likely to continue. Indeed, Trump's initial aggressive actions toward a number of traditional U.S. allies, such as his threats of tariffs against Canada and European countries, risk elevating allied concerns that Trump could weaponize their dependence on U.S. technology against them and encouraging allies to more aggressively reduce their own use of U.S. technology. This makes proactive engagement even more important.

Historical Background

The specific risks the United States faces from China's access to data and control of software and connected devices are a product of the twenty-first century. Before the creation of the World Wide Web in 1989, there was no meaningful public internet or readily accessible online data, and "connected devices" meant government and university computer servers attached to early U.S. government IT networks like ARPANET. It was not until the 2000s that Chinese companies became significant players in designing and manufacturing high-tech products like telecommunications network infrastructure equipment, electric vehicles, and social media platforms. Indeed, in the years following the global spread of the internet in the 1990s, U.S. officials generally argued against foreign government plans to restrict international data flows and to close markets to software and connected devices, arguing that an open internet would advance both American values and American commercial interests, given the dominant role that U.S. companies played in the tech sector.

Even though the specific risks associated with China's access to data and control of software and connected devices are new, the underlying concerns about foreign control of U.S. infrastructure and ability to influence U.S. opinion are not. More than two centuries ago, in the aftermath of the War of 1812, Congress passed a law restricting foreigners from owning ships that sailed between American ports, hoping both to strengthen U.S. industry and to ensure that foreigners could not control America's domestic trade.[31] At the dawn of America's commercial aerospace industry in the 1920s, Congress extended ownership restrictions to airlines, in part out of concern that foreign companies flying aircraft over the U.S. heartland could hurt U.S. national security.[32]

American concern about foreign ownership of communications networks and broadcast media similarly emerged during the first decades of wireless communications. In the early 1900s, the U.S. Navy became concerned that foreign spies could use the then-new medium of radio to send information abroad and to direct military attacks during a time of war. In

1912, at the Navy's behest, Congress prohibited foreign nationals from acquiring or owning radio broadcast licenses in the United States.[33] Many decades later, in 1985, laws restricting foreign ownership of U.S. broadcast television licenses forced Australia media baron Rupert Murdoch to become a U.S. citizen before he could buy the stations that become the foundation for his U.S. television empire.[34]

The United States has never directly imposed foreign ownership prohibitions on print media, but there is a long history of laws trying to ensure that American print media was free of foreign influence. During World War I, the Trading with the Enemy Act required German-language newspapers to file English translations of their publications with the postal service, and the post office could refuse to mail publications it deemed to support Germany. During the 1930s, the U.S. government passed the Foreign Agent Registration Act in an attempt to require pro-German propagandists and publications to register as agents of the German government. Even today, the Committee on Foreign Investment in the United States (CFIUS), a Treasury-led process that reviews foreign acquisitions of U.S. companies for national security risks, can limit foreigners trying to buy U.S. media properties. In 2023, for example, CFIUS scrutiny contributed to the collapse of a planned buyout of *Forbes* magazine.[35] Similarly, German publisher Alex Springer had to address CFIUS issues when it bought *Politico* in 2021.[36]

The United States began imposing restrictions on foreign ownership of telephone networks in the 1930s. The first comprehensive U.S. communications law, the Communications Act of 1934, included provisions prohibiting foreigners from owning more than 20 percent of most U.S. "common carrier" phone and telegraph companies. The Federal Communications Commission (FCC) has for decades required companies that want to offer telecommunications services between the U.S. and foreign countries to obtain licenses.[37]

Evan when the United States liberalized its domestic telecommunications markets in the 1990s, it retained the authority to limit foreign ownership if it identified a specific national security risk. For example, the United States pledged to end most *per se* statutory prohibitions on foreign investment in U.S. telecommunications markets as part of its 1997 commitments to join the World Trade Organization.[38] But the FCC simultaneously created a new government body, known as "Team Telecom," that tapped U.S. national security agencies to review the national security risks associated with foreign investments in U.S. telecommunications and applications to provide telecom services to Americans.[39]

Against this historical backdrop, U.S. government concerns about Chinese access to data and control of software and connected devices first seriously emerged in 2005, when a little-known Chinese computer company, Lenovo, struck a deal to acquire IBM's legendary but low-margin PC division—a deal that would give a Chinese company control over computers and laptops used in businesses, schools, and government agencies. CFIUS ultimately

approved the deal but only after imposing "mitigation measures" to address potential security risks, such as requiring the physical separation of Lenovo employees working on PCs from IBM employees who would continue to work on more sensitive servers and other products.[40]

In the years following that 2005 case, CFIUS emerged as a major tool in U.S. government efforts to limit China's access to U.S. data and software. Publicly reported CFIUS cases involving Chinese access to data and software over the past two decades include acquisitions of U.S. computer server companies, a U.S. health data company, LGBTQ dating app Grindr, money transmitter MoneyGram, and the insurance industry, among others.[41] At times, CFIUS blocked takeovers or required a Chinese buyer to divest U.S. operations that a Chinese company had already acquired. At other times, as it had in 2005, CFIUS approved a transaction but required measures to mitigate risks. Though CFIUS does not publish the terms of specific deals, a review of its public annual reports over the past fifteen years indicates that mitigation measures can include limiting access to company and customer data to specific employees or to U.S. citizen employees (for example, no Chinese parent company or Chinese national access to the data); establishing security committees to limit access to sensitive technology and data; ensuring that certain products remain in the United States; and ensuring that only authorized vendors provide the U.S. company with certain products and services.

By the late 2000s and early 2010s, however, American national security officials began to encounter the limits of CFIUS. CFIUS can block a Chinese acquisition of a U.S. company that holds American data or develops software or devices, but it has no authority to block U.S. companies from selling data to China or purchasing Chinese technology, or to prevent Chinese companies from simply directly marketing their products to Americans. With Chinese companies playing an increasing role in global markets, U.S. policymakers began seeking new tools to address perceived risks.

At first, these tools focused on informal pressure on the corporate sector and on information gathering. In 2010, for example, Secretary of Commerce Gary Locke called the CEO of mobile carrier Sprint to urge that Sprint not consider a bid from Chinese national champion telecommunication company Huawei to perform extensive upgrades to Sprint's telecommunications networks in the United States.[42] The following year, realizing that it did not know the extent to which Chinese equipment already had been installed in U.S. telecommunications networks—particularly by smaller, rural telecommunications companies—the Obama administration used a Cold War–era law to require U.S. telecoms providers to report on Chinese networking equipment installed in U.S. networks.[43]

After Trump was inaugurated in 2017 and identified China as America's chief economic and strategic competitor, congressional and executive branch officials began to develop a more formal regulatory apparatus to address perceived risks posed by China's access to data and its ability to exploit Chinese-owned software and connected devices. The initial focus was on telecommunication network infrastructure: Trump officials expressed concern about

the risk that China could exploit its telecommunications gear to spy on U.S. citizens and to engage in industrial espionage in the United States.[44] In response, the Trump administration launched domestic and international campaigns to reduce the use of Chinese equipment in telecommunications networks.[45] The government also became increasingly concerned about the its own reliance on other types of Chinese equipment that China potentially could use to conduct espionage. In 2018, for example, Congress prohibited the use of many Chinese surveillance cameras at U.S. government facilities and directed the government to establish the Federal Acquisition Security Council (FASC) to review the security risks associated with U.S. government procurement of information communications technology software and devices.[46]

By 2019, the government was concerned not only about telecommunications networks and the government's infrastructure, but also about American private sector uses of Chinese-connected technologies. In May 2019, Trump signed Executive Order (E.O.) 13873, which directed the Commerce Department to set up a process to review and address risks in America's information and communications technology supply chain (ICTS), including potentially restricting Chinese software and devices.[47] As then commerce secretary Wilbur Ross said when the executive order was announced, the goal was to ensure that "Americans will be able to trust that our data and infrastructure are secure."[48] In March 2020, Congress passed the Secure and Trusted Communications Networks Act of 2019, which directed the FCC to maintain a public list of communications equipment and services that posed an unacceptable risk to U.S. national security.

The pace of rules and regulations increased during Trump's final months in office, notably with new executive orders that sought to ban TikTok and nine other Chinese apps from being distributed in the United States. Although those bans were enjoined by courts and ultimately did not come into effect, they were a precursor for more recent actions, including Congress's TikTok divestment law in 2024. Appendix A provides a timeline of major Trump administration actions.

Although Biden had been critical of aspects of Trump's policy toward China while on the campaign trail in 2020, the Biden administration steadily—and in 2024 substantially—expanded the regulatory regime it inherited from Trump. In June 2021, while withdrawing the Trump administration's court-blocked executive order attempting to ban Chinese apps, Biden issued E.O. 14034, which expanded on Trump's ICTS executive order by directing the Commerce Department to evaluate Chinese software and connected devices for security risks and to take steps to mitigate identified risks.[49] In November 2021, Biden signed the Secure Equipment Act of 2021, which authorized the FCC to effectively ban internet-connected products that it determined threaten U.S. national security and not simply to maintain a public list. A year later, in November 2022, Biden's FCC used that authority to ban new security cameras made by two Chinese companies from being connected to the internet in the United States, effectively banning their sale or use.[50]

In 2024, the Biden administration and Congress took additional steps to begin restricting data flows to China and to address the risks associated with Chinese software and connected devices. Some of these involved bureaucratic changes to support the U.S. government's work. In early 2024, the Commerce Department hired former Microsoft executive Liz Cannon to run a newly established Office of Information and Communications Technology Services that would implement Commerce's authorities over the ICTS supply chain.[51] Other measures involved new restrictions on Chinese data flows, software, and connected technologies. In February 2024, Biden signed a new executive order to address cybersecurity risks at U.S. ports, and the U.S. Coast Guard issued a directive to U.S. port operators directing them to address security risks associated with their use of Chinese-manufactured cargo cranes, which U.S. defense officials previously had raised as a concern.[52] Less than a week later, Biden signed E.O. 14117, which directed the Justice Department to establish regulations restricting data brokers from selling or transferring multiple different types of data to China and to Chinese companies in instances where doing so could impact U.S. security.[53]

Two months later, in April, Congress passed a bill that would give ByteDance until early 2025 to divest its ownership of TikTok; failure to do so would mean that TikTok would face a ban on distribution through U.S. app stores. On January 20, 2025, Trump announced that he would seek to extend the deadline by seventy-five days to give his administration additional time to work out a deal, but Trump continues to indicate that he expects TikTok to be at least 50 percent owned by Americans. Congress's April 2024 law also authorizes the government to impose similar divestment restrictions on other widely used Chinese social media apps, and to ban apps that do not comply with a divestment order.[54] And as with E.O. 14117, this law included Federal Trade Commission (FTC) enforcement provisions to prohibit data brokers from selling personally identifiable information to China.[55]

Also in 2024, the Biden administration announced plans to restrict the sale of internet connected cars manufactured in China, citing the national security risks that such cars could pose on U.S. roads, and it finalized the rules in early 2025.[56] The Biden administration also launched a process in early 2025 that, if continued by Trump, could result in a ban on Chinese-made drones in the United States, in light of potential security risks.[57] Appendix B provides a timeline of significant Biden administration actions to address the risks associated with Chinese access to U.S. data and Chinese software and connected devices in the United States.

Additional measures reportedly are under consideration. In a trade policy executive order that Trump signed on his second Inauguration Day, Trump directed his commerce secretary to "consider whether controls on ICTS transactions should be expanded to account for additional connected products."[58] Meanwhile, the leadership of the U.S. House of Representatives Select Committee on the Chinese Communist Party has urged the executive branch to examine and address security risks posed by Chinese cellular modules, Wi-Fi routers, drones, and semiconductors.[59]

The Emerging U.S. Regulatory Regime

This decade-plus of U.S. government work to address the risks posed by China's access to data and control of software and connected technologies has created a growing array of regulatory authorities. These authorities regulate Chinese software; Chinese devices, and technologies that connect to the internet; Chinese telecommunications companies that connect to the United States; and the flow of American data to China. They are spread across multiple agencies, including the Commerce Department, the Justice Department, the FCC, and the Department of Homeland Security. Some of the authorities consist of formal rules and regulations; others are voluntary standards and awareness-raising efforts by the U.S. government intended to influence private sector decisions without directly regulating them. Core elements of the existing regulatory regime include the following:

- ***The Commerce Department's ICTS authorities to restrict the distribution and use of information and communications technology and software:*** Two executive orders, E.O. 13873 on the information and communications technology supply chain and E.O. 14034 on foreign adversary controlled apps and software, empower the Commerce Department to review and address risks associated with information and communications technology and services and/or software applications designed or developed by designated "foreign adversary" countries, which currently is defined to include China, Russia, and several other countries.[60] These executive orders empower the department to review the risks associated with a broad range of technologies, including network infrastructure equipment, software, and devices that connect to the internet, and to impose restrictions or mitigation measures to address identified security risks. The department issued its first major restriction pursuant to these authorities in June 2024, when it banned the U.S. distribution and sale of software made by Russia cybersecurity firm Kaspersky Labs.[61] In September 2024, the department published a draft rule restricting the sale of Chinese autonomous driving technology in the United States as well as cars using certain Chinese connectivity modules.

- ***The Federal Communications Commission's "Covered List," which effectively prevents covered items and services from connecting to U.S. communications networks or internet:*** The FCC maintains a "Covered List" of items or services "deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[62] Pursuant to the Secure Equipment Act of 2021, as of February 2023, the FCC will deny authorizations to equipment and services on the Covered List, meaning that the equipment cannot connect to U.S. telecommunications networks. This denial effectively prohibits covered devices, software, or telecommunications services from being used in the United States. The FCC does not make its own independent decisions on whether to include specific equipment or services on the Covered List, but instead takes direction from relevant national security agencies. For example, when the FCC

added two Chinese telecommunications providers to the Covered List in September 2024, it stated that it did so at the request of the Department of Commerce and with the concurrence of the Department of Justice and Department of Defense.[63] The Covered List currently restricts several types of Chinese telecommunications network infrastructure, several Chinese security cameras, Kaspersky software, and several Chinese telecommunications services.

- ***The Commerce Department's "Know Your Customer" requirements for U.S. cloud services providers:*** In January 2024, the Commerce Department proposed a rule that would require companies providing internet infrastructure as a service—effectively, cloud services providers—to establish KYC rules that would enable them to identify their customers and the owners of their customers.[64] The intent of the rule is to help U.S. companies and ultimately the U.S. government to better identify and cut off foreign companies and entities that use cloud services to support espionage and other malicious cyber activity.

- ***"Team Telecom" to prevent high-risk communications companies from operating in the United States or connecting to U.S. networks:*** The FCC's "Team Telecom" process reviews applications by foreign companies to start offering communications services in the United States or to offer international communications services (such as via submarine telecommunications cables) to the United States. In recent years, it has denied authorizations to China-linked companies while also requiring a planned Google- and Meta-operated cable that had a Chinese partner to adopt measures to mitigate potential data security risks.[65]

- ***The Department of Justice's "Data Security" executive order that authorizes the department to limit bulk data transfers to China:*** Pursuant to E.O. 14117, the Department of Justice is drafting rules to prohibit or otherwise restrict the transfer of certain U.S. government or U.S. bulk data to China and other jurisdictions deemed to pose a threat. The department's authority includes both the ability to regulate only arms-length sales or transfers of sensitive U.S. data to China, and to restrict vendor agreements between U.S. firms and Chinese companies that could provide the Chinese companies with access to the data, such as an agreement between a U.S. hospital chain and a Chinese firm to process U.S. patient data. The data transfer rules also effectively may limit the deployment of certain Chinese software and connected devices in the United States, given that many types of software and connected devices collect data—particularly personal information and geolocation data—that a Chinese company ordinarily would process back in China.

- ***The Federal Trade Commission's enforcement of the Protecting Americans' Data from Foreign Adversaries Act:*** In April 2024, Congress enacted the Protecting Americans' Data from Foreign Adversaries Act, which prohibits data

brokers from selling certain categories of U.S. individuals' personally identifiable sensitive information to China or to Chinese companies. This law overlaps significantly with but is also distinct from and in some ways broader than Biden's 2024 data security executive order.[66]

- ***The Committee on Foreign Investment in the United States:*** CFIUS continues to have authority over foreign acquisitions of U.S. companies that control telecommunications or other key infrastructure or that hold sensitive U.S. data, including the authority to mandate mitigation measures and to recommend that the president block acquisitions outright. In 2018, Congress amended the CFIUS statute to increase the committee's focus on sensitive data (among other reforms). In 2022, Biden issued an executive order directing CFIUS to increase its focus on data security risks as well as several other national security concerns.[67]

- ***Congress's divestiture requirements for Chinese-owned social media companies:*** In April 2024, Congress enacted legislation to prohibit app stores from distributing popular social media app TikTok starting in early 2025 unless TikTok's Chinese parent, ByteDance, divested itself of the company. The same legislation authorized the president to impose a similar divestment requirement or distribution ban for other Chinese social media companies that have more than 1 million U.S. users and which the president determines pose a threat to U.S. national security.[68] This requirement could impact fast-growing Chinese social media companies such as MiniMax and Hypic.[69] (On January 17, 2025, the Supreme Court upheld the constitutionality of the law.[70])

- ***The Federal Acquisition Security Council and other federal procurement restrictions:*** The Office of Management and Budget (OMB) chairs the FASC, which Congress chartered in 2018. The FASC consists of key security and procurement agencies. Its mandate is to reduce cybersecurity and supply chain risks in federal procurement, including the risks posed by foreign ownership or control of an item that the government is buying. It has the authority to prohibit the federal government from purchasing specified products and, in particularly high-risk instances, to order the "rip and replace" of software and other equipment already in federal systems. Although FASC decisions are limited to restrictions on federal procurement, FASC restrictions generally also will be noticed publicly, potentially sending a signal to private sector purchasers as well.

Beyond the FASC, the government has other authorities to regulate its own procurement of high-risk products. One such example is the Department of Homeland Security's authority to issue "Binding Operational Directives" to agencies to mitigate identified cybersecurity risks.[71] Moreover, Defense Department procurement regulations prohibit it from purchasing goods made by Chinese companies that the department has identified as part of China's military-industrial complex.

- ***Sectoral regulators:*** Although the United States does not have a cross-cutting cybersecurity regulator, several sectoral regulators have the potential to impose restrictions on the use of Chinese software and connected technology if they determine that such products or services threaten the integrity of networks or undermine U.S. security. For example, in February 2024 the U.S. Coast Guard, which has regulatory authority over ports and shipping, issued a maritime security directive on the security risks posed by use of Chinese-made port terminal cargo cranes and directed port operators to take steps to address these risks.[72] Federal regulators overseeing the banking and healthcare sectors also have the authority to direct regulated companies to take steps to ensure appropriate cybersecurity protections that will restrict regulated entities from transmitting data to China and from relying on Chinese software and connected technologies. For example, in December 2024 the Consumer Financial Protection Bureau proposed rules that will prohibit data brokers from selling certain financial information in support of efforts to protect sensitive U.S. data from foreign adversaries.[73] The U.S. Treasury Department and Federal Reserve have authorities to mandate that financial institutions impose data security measures, while the Department of Health and Human Services has some authorities to ensure the protection of U.S. health data.

Beyond these core regulatory authorities, the U.S. government has other tools at its disposal to address the risks posed by data transfers to China and by Chinese control of software and connected devices. These include awareness-raising efforts to ensure that the U.S. private sector and U.S. citizens understand relevant risks, mechanisms to leverage private sector guidance documents and standards, and the Commerce Department's authority to restrict imports that threaten U.S. national security.

- ***Department of Homeland Security and law enforcement awareness-raising efforts:*** The Department of Homeland Security, the Federal Bureau of Investigation (FBI), and U.S. intelligence agencies possess only limited regulatory authority over the use of Chinese software and connected technology in the United States, but they do have tools to raise public and business awareness of potential risks. Earlier this year, for example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued a formal warning to companies operating critical infrastructure about the risks associated with using certain Chinese-connected devices, such as drones.[74] FBI field offices can engage with local companies to discuss potential espionage and cybersecurity risks. And the Director of National Intelligence has published a summary document describing Chinese laws that could compel Chinese companies to cooperate with national security and intelligence work—a type of public outreach that could be expanded.[75]

- ***Voluntary cybersecurity standards:*** The U.S. National Institute of Standards and Technology publishes a national Cybersecurity Framework that provides guidance to U.S. businesses, including small businesses, on cybersecurity best practices and ways to identify and address cybersecurity risks. Other agencies, including the Cybersecurity and Infrastructure Security Agency, promote voluntary cybersecurity standards for companies that operate critical infrastructure across a range of sectors. To date, these standards have not incorporated specific risks related to data transfers to China or use of Chinese software or connected technology, but they do provide guidance on a wide range of more general cybersecurity risks and best practices.

- ***The Commerce Department's "Section 232" authorities:*** Section 232 of the Trade Expansion Act of 1962 authorizes the Commerce Department to regulate imports of products when the department determines that imports threaten to impair U.S. national security. The department historically has used Section 232 to protect U.S. manufacturing: Trump, for example, used Section 232 to regulate U.S. imports of steel. The Commerce Department could leverage these authorities to restrict imports of products where the product itself was determined to create a national security risk: at least one outside assessment, for example, has noted that the department could use Section 232 to impose tariffs or other import restrictions on U.S. imports of Chinese semiconductors if it determined that the semiconductors posed a threat to U.S. national security.[76]

- ***Federal Trade Commission authorities:*** Finally, the FTC has general authority to act against unfair and deceptive trade practices, including by tech companies. In recent years, for example, the FTC has taken action against companies that do not honor the privacy commitments they make in their own terms of service, and the FTC recently warned companies against deceptively changing their terms of service to allow themselves to exploit user data to train AI models.[77] The FTC potentially could use its authorities to penalize a Chinese company that shared information with the Chinese government without adequate user consent.

Policy Recommendations

As the history and regulatory authorities described in this paper illustrate, over the past decade—particularly since the late 2010s—the United States has developed a surprisingly complex regulatory regime to restrict data transfers to China and to address the risks posed by Chinese software and connected technology. This regime has potentially profound significance for the U.S.-China relationship, given that a growing share of U.S.

imports—including even household and consumer devices like kitchen appliances and lighting systems—connect to the internet, creating security vulnerabilities and potentially subjecting them to regulation. Chinese tech startups, as well as established companies like Temu and Shein, remain focused on the United States as a potential market and almost will certainly find themselves subject to increased U.S. government scrutiny and regulatory pressure. China's parallel regulatory regime to address the risks Beijing assesses it faces from reliance on U.S. tech will have similarly significant impacts on U.S. companies operating in the world's second-largest economy. And, as governments around the world begin to develop their own measures to reduce data, software, and connected device risks, the United States will need to ensure that those measures address legitimate security risks posed by China without adversely impacting U.S. firms.

Pressure to use these authorities to further restrict U.S. data flows to China and the operations of Chinese software and connected devices in the United States almost certainly will increase over the coming years, driven by intense Sino-U.S. geopolitical competition and continued American concern about Chinese cyber risks to the United States. As the United States continues to develop its regulatory regime for U.S.-China data flows and for Chinese software and connected devices, policy recommendations include the following:

Embed China-focused measures within a broader set of measures to improve data privacy and cybersecurity. China's sophisticated hacking operation has multiple avenues to exploit U.S. data, influence U.S. opinion, and breach U.S. networks without relying on Chinese companies obtaining direct access to U.S. data or controlling software or technology. The United States cannot effectively protect against China-related data, influence, and cybersecurity risks without adopting broader and more comprehensive measures to protect Americans' data and to enhance U.S. cybersecurity. Indeed, recent events have illustrated this fact: While the United States took steps in the late 2010s to limit the use of Chinese telecommunications network infrastructure equipment in U.S. telecommunications networks, over the past several years China mounted a sophisticated hacking program into U.S. telecoms networks—providing vast and unprecedented access to Chinese spies, including to the communications of senior U.S. government officials.[78]

A U.S. national data privacy law that limits data collection in the first place, for example, would limit the pools of sensitive American data that China potentially could hack regardless of whether they are held by U.S. or Chinese firms—not to mention the domestic privacy benefits. A national data privacy law would also have domestic privacy benefits and help align U.S. policy with allied nations that have strong privacy protections. A strong national data privacy law and cybersecurity measures should be the government's primary focus, with measures specifically targeting data transfers to China and Chinese software and connected devices playing an important supporting role.

Publish a formal risk assessment and strategy for the government's work. The U.S. government should publish a comprehensive assessment of the risks posed by China's access to U.S. data and control of software and connected technologies and a strategy to address

those risks, publicly including specific priority areas for U.S. government focus. In 2024, the Commerce Department published a list of priority technologies it is focused on, pursuant to authorities limiting Chinese software and connected technology in the United States, which could serve as a partial basis for a broader cross-U.S. government strategy.[79] However, the U.S. government has not published an overarching strategy identifying specific cross-cutting technologies of concern; describing when it will seek to mitigate risks with regard to blocking data transfers, software, and connected devices; or describing cross-cutting steps that it would like to see U.S. private sector companies take to begin addressing risks on its own. A formal U.S. government risk assessment and strategy would harmonize work across agencies while providing a signal to the U.S. private sector of specific priority areas to reduce reliance on Chinese software and connected technologies.

Develop clear guidelines for assessing risks: Different government agencies and authorities have established overlapping but also somewhat different criteria for evaluating the risks posed by China's access to data and its control of software and connected technologies. Some tools, such as the FCC's Covered List, do not appear to be guided by published risk criteria at all. As part of its published risk assessment and strategy, the government should publish a clear set of the criteria it uses and recommends that private entities use these criteria to assess the risks associated with data transfers to China and use of Chinese software and connected technology. Such criteria could include the following elements:

- Data sensitivity and volume
- Ownership or control of companies with access to data and control of software and connected devices
- Whether software or a device is intended to be used to for sensitive applications, such as critical infrastructure
- The scale of use or dependency—for instance, is it widely used, or is it one of several similar products that also are being used and could be substituted if necessary?
- The potential for software or a connected device to be used to mount attacks or facilitate influence campaigns
- The ease of replacing software or devices—for instance, the difficulty of "rip and replace" if subsequent risks are identified
- The ability to provide software updates not subject to oversight, including whether malware could be inserted
- The extent of involvement of trusted parties in the development and distribution of the software or connected device, such as whether a third party can monitor for potential malicious activity

- The availability of mitigation options such as encryption, data localization, technical reviews of code, and independent monitoring and oversight

These criteria should be updated as risk perceptions evolve.

Develop clear principles to guide the development and deployment of software and connected device restrictions: While the United States has a compelling interest in imposing sensible restrictions on the use of high-risk Chinese software and connected devices, it also has a compelling interest in both avoiding broader-than-necessary restrictions and in avoiding setting a precedent that foreign governments skeptical of U.S. technology firms could use to impose their own national restrictions on the use of U.S. technology. The United States can balance these interests by developing and publishing a clear set of principles to guide the deployment and development of restrictions on Chinese software and connected devices. Articulating clear principles can help limit the potential overuse of restrictions by U.S. agencies as well as providing a framework for international cooperation with allies and partner nations.

Improve information disclosure and monitoring. Although U.S. government officials have spoken publicly about the risks of data flows to China and Chinese control of software and connected technology, they generally have not disclosed specific instances of China's use of its software or connected devices for harmful purposes. Moreover, the U.S. government appears to have little systematic information regarding the extent of data transfers to China or the prevalence of Chinese software and connected technology in the United States beyond high-profile examples such as TikTok and Chinese automobiles. Closing this information gap will be essential to effective policymaking. The Commerce Department could, for example, conduct a survey of various U.S. critical infrastructure companies to determine the extent to which they are using Chinese software or connected devices in their networks. It also could require Chinese companies selling certain types of technology in the United States to file a notice with the U.S. government so that the government understands their role in the market. The U.S. government may also consider expanding the KYC requirements that currently apply to cloud services providers to app store providers to ensure that major software distributors (and their customers) in the United States know if they are distributing Chinese technology.

Develop standards for mitigation measures. Mitigation measures likely will play an important role in addressing China-related data security, software, and connected device risks. A Chinese-designed home vacuum cleaner robot, for example, might be able to collect substantial sensitive information, including interior maps of the homes of government officials and corporate executives. Those risks, however, could be mitigated with technical solutions that prevent customer data from traveling to China and third-party auditing of software to ensure that malicious code is not inserted. Over more than three decades, the CFIUS process has developed a set of mitigation measures that can reduce the risks associated with a foreign takeover of a U.S. company, with CFIUS blocking transactions only in particularly

high-risk scenarios. The United States should develop and promote mitigation measures to reduce the risks of less risky Chinese products, while reserving bans for higher-risk products and applications.

Codify the executive branch's authorities. Both the Trump and Biden administrations have relied heavily on a 1970s statute, the International Emergency Economic Powers Act (IEEPA), as the legal basis for limiting certain data flows to China for regulating certain Chinese software and connected devices in the United States. IEEPA, for example, forms the basis of both Trump's ICTS executive order and Biden's software executive order. IEEPA, however, was drafted before the internet existed and does not, for example, clearly authorize the government to impose all of the mitigation measures that policymakers might want to pursue. Moreover, there are limits to IEEPA's reach: in 2020, when the Trump administration sought to use IEEPA to ban TikTok, U.S. courts concluded that IEEPA did not grant the executive branch the authority to impose such a ban. Given recent U.S. court rulings holding that major policies should be clearly authorized by Congress, Congress should codify authorities to regulate in this area both to provide a sound statutory basis and to provide appropriate oversight of executive branch policymaking.

Develop international standards with like-minded allies: The United States has both an interest and an opportunity to collaborate with like-minded allies in the development of shared approaches to the regulation of Chinese access to data and control of software and connected devices. Shared approaches to standards will reduce the risks that U.S. allies and partners will find themselves dependent on Chinese software and connected devices and that U.S. allies, concerned about their own vulnerabilities, will impose restrictions of their own on both Chinese and U.S. firms. Moreover, key allies appear to be interested in joint approaches: Japan has been promoting its "data free from with trust" framework for several years, while both U.S. and European Union officials are developing labeling programs to label connected devices that meet cybersecurity standards. The United States should launch a new initiative to cooperate with allies to establish joint approaches to addressing the risks of data flows to China and of Chinese-controlled software and connected devices.

Conclusion

In 2000, as China was embarking on a multidecade process to crack down on domestic internet usage, then president Bill Clinton jokingly wished Beijing well. "Good luck," he quipped. "That's sort of like trying to nail Jell-O to the wall." But over the ensuing decades, China did largely succeed in regulating its domestic internet economy, developing systematic censorship, building national champion enterprises, and restricting many major Western firms from entering its market. The United States, meanwhile, remained open to China, not

just for information from and about China—openness that the United States should always value—but also open to a growing array of cross-border data flows, Chinese software, and connected devices.

The United States should not follow in China's model: its open society is a national strength. Moreover, unduly broad restrictions on Chinese companies' access to data and on Chinese software and connected technology in the United States could have adverse unintended consequences: disrupting ordinary commercial trade that depends on data flows, for example, or reducing beneficial innovation because U.S. firms are not exposed to competition from Chinese competitors. But in today's era of strategic competition, United States policymakers need to address the data security, disruption, and influence risks that come from cross-border data flows, Chinese software, and connected devices. Since the 2010s, they have begun to do so, with dozens of actions involving myriad government agencies. Now, government policymakers need to develop a more systematic and comprehensive framework for managing the relationship going forward.

Appendix A: Timeline of Trump Administration Actions on U.S.-China Data Flows, Software, and Connected Equipment

2017 Congress enacts legislation prohibiting Defense Department procurement of Huawei telecommunications equipment for use in certain networks, expanded in 2019 to cover all U.S. government agency procurement.[80]

2018 Congress enacts legislation prohibiting the use of certain Chinese security cameras at sensitive U.S. government sites.[81]

2018 The Federal Communications Commission (FCC) proposes rules to prohibit telecom companies that receive FCC grants to support service in rural and underserved areas from using the grants to procure equipment from Huawei, ZTE, and other Chinese telecommunications equipment. (The rules were finalized in 2019.)[82]

2018 Congress enacts the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), which directs the U.S. government to establish procedures to limit data and cybersecurity risks associated with U.S. government procurement.[83]

2018 The Trump administration launches an international campaign to encourage U.S. allies and partners to restrict the use of Huawei and other Chinese telecommunications equipment in their network infrastructure, effectively taking U.S. concerns global.[84]

2019 Trump issues E.O. 13873, which directs the Commerce Department to set up a process to identify security risks in the information and communications technology supply chain (ICTS) and to mitigate identified risks by, for example, excluding certain devices from U.S. telecommunications networks. [85]

2019 The Commerce Department puts Huawei on the Entity List, prohibiting many U.S. exports to the company.[86]

2019 The FCC denies a long-pending application by the Chinese telecom firm China Mobile International to offer telecommunications services in the United States.[87]

2019 The Interior Department prohibits its components from purchasing Chinese-made drones.[88]

2020 Congress enacts the Secure and Trusted Communications Networks Act of 2019, which directs the FCC to maintain a public list of communications equipment and services "deemed to pose an unacceptable risk to the national security of the United States"—the so-called Covered List.[89]

2020 Citing data security concerns, the Trump administration recommends that the FCC deny authorization for a submarine internet cable connecting the United States to Hong Kong.[90]

2020 Trump issues a set of executive orders intended to ban TikTok and Chinese messaging app WeChat.[91] These orders would be enjoined by U.S. courts at a later date.

2020 The State Department launches a short-lived "Clean Network" initiative to promote limits on Chinese telecommunications networks, telecommunications cables, cloud services, and apps globally.[92]

2021 Trump issues an executive order to ban Chinese payments app AliPay and seven other Chinese apps.[93]

2021 Trump signs an executive order directing the Commerce Department to establish regulations to address malicious cyber actors' use of U.S. infrastructure as a service provider.[94] This order would become the basis for the "Know Your Customer" rules released by the Biden administration in 2024.

Appendix B: Timeline of Biden Administration Actions on U.S.-China Data Flows, Software, and Connected Equipment

2021 President Joe Biden signs Executive Order 14034, authorizing the Commerce Department to evaluate Chinese software and connected devices for security risks and to take steps to mitigate identified risks.[95]

2021 The Federal Acquisition Security Council issues a final rule on how it will review security risks associated with federal procurement, including risks related to foreign control or influence over the maker of software or a device.[96]

2021 and 2022 Biden's Federal Communications Commission (FCC) revokes two existing authorizations for Chinese companies to offer telecommunications services in the United States.[97]

2021 Congress passes the Secure Equipment Act of 2021, which requires the FCC to effectively ban U.S. sales of products and services on the FCC's Covered List—a list of communications products and services the FCC determines pose an unacceptable risk to U.S. national security.[98]

2022 The FCC issues the first bans under the Secure Equipment Act, effectively prohibiting the sale of new security cameras made by Chinese companies Hikvision and Dahua, as well as telecommunications equipment made by several other Chinese companies.[99]

2023 The Commerce Department publishes a rule explaining how it would implement Executive Order 14034 and spelling out the criteria it would use to evaluate the risks associated with covered Chinese software and devices.[100]

2023 The Commerce Department announces an industrial base survey to understand the sourcing of mature node semiconductors in the United States in order to identify potential China supply chain risks.[101]

2024 The Department of Homeland Security and the Federal Bureau of Investigation issue a public advisory, warning critical infrastructure providers about the risks of using Chinese drones.[102] (As of September 2024, the Commerce Department reportedly is considering a rulemaking process to formally limit their use.)

2024 The Commerce Department issues a draft rule directing cloud services providers to establish "Know Your Customer" standards for their foreign customers.[103]

2024 Biden directs the Coast Guard to issue guidance to reduce the security risks associated with using Chinese made cranes at U.S. ports, while also announcing a program to begin building cranes in the United States.[104]

2024 The Commerce Department announces its first major action pursuant to Executive Order 14034, a rulemaking process that will restrict the use inside the United States of Chinese cars capable of connecting to the internet (which includes most modern cars, given that most modern cars connect to the internet for mapping, software updates, and other purposes).[105]

2024 Biden signs Executive Order 14117, directing the Department of Justice to establish rules restricting the bulk transfer of certain sensitive U.S. information to China, Russia, and other adversarial nations.[106]

2024 Congress enacts legislation to force Chinese company ByteDance to divest its TikTok social media app or else see a ban on the distribution of TikTok in the United States. The same law also directs the divestment or blocking of U.S. distribution of other Chinese-owned social medial apps, websites, and software products that have 1 million or more U.S. monthly active users.[107]

2024 Congress enacts legislation prohibiting U.S. data brokers from transferring the "personally identifiable sensitive data of a United States individual" to China or a Chinese company, and charges the Federal Trade Commission with enforcement.[108]

2025 The Commerce Department issues an Advanced Notice of Proposed Rulemaking to address security risks posed by Chinese-made drones in the United States.[109]

About the Author

Peter E. Harrell is a nonresident fellow at the Carnegie Endowment for International Peace. He also serves as an attorney advising companies and investors on international legal, regulatory, and geopolitical risks. As a member of Carnegie's American Statecraft program, Harrell's research focuses on issues of U.S. domestic economic competitiveness, trade policy, and the use of economic tools in U.S. foreign policy.

Notes

1 See, for instance, Hung Tran, "Dual Circulation in China: A Progress Report," Atlantic Council, October 24, 2022, https://www.atlanticcouncil.org/blogs/econographics/dual-circulation-in-china-a-progress-report/.

2 White House, "National Security Strategy," December 2017, 2, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

3 President Joe Biden, "Introduction to the National Security Strategy," White House, October 12, 2022, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.

4 Sam Sabin, "Why China Hawks Care So Much about Cranes," Axios, September 17, 2024, https://www.axios.com/2024/09/17/chinese-cargo-cranes-secruity-risks.

5 See Center for Strategic and International Studies (CSIS), "Significant Cyber Incidents Since 2006," https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

6 Christopher Bing, "FBI Says Chinese Hackers Preparing to Attack US Infrastructure," Reuters, April 18, 2024, https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/.

7 See Sarah Friedman, "United States: Appeals Court Rules on Chinese Manufacturers' Challenge to FCC Order Implementing Secure Equipment Act," Library of Congress, April 17, 2024, https://www.loc.gov/item/global-legal-monitor/2024-04-16/united-states-appeals-court-rules-on-chinese-manufacturers-challenge-to-fcc-order-implementing-secure-equipment-act/.

8 See Robert McCartney and Faiz Siddiqui, "Could a Chinese-made Metro Car Spy on Us? Many Experts Say Yes," *Washington Post*, January 7, 2019, https://www.washingtonpost.com/local/trafficandcommuting/could-a-chinese-made-metro-car-spy-on-us-many-experts-say-yes/2019/01/07/00304b2c-03c9-11e9-b5df-5d3874f1ac36_story.html.

9 See, for instance, Tiffany Hsu, "Chinese Influence Campaign Pushes Disunity Before U.S. Election, Study Says," *New York Times*, February 15, 2024, https://www.nytimes.com/2024/02/15/business/media/chinese-influence-campaign-division-elections.html.

10 Hannah Rabinowitz and Evan Perez, "Justice Department Responds to TikTok Lawsuit, Argues Algorithm Could Allow Chinese Government to Influence US Elections," CNN, July 27, 2024, https://www.cnn.com/2024/07/27/tech/tiktok-response-to-us-ban/index.html.

11 See Julien E. Barnes, "China Could Threaten Critical Infrastructure in a Conflict, N.S.A. Chief Says," *New York Times*, April 17, 2024, https://www.nytimes.com/2024/04/17/us/politics/china-cyber-us-infrastructure.html.

12 See, e.g., Andrew Grotto, Cyber Security Derailed? Recommendations for Smarter Investments in Infrastructure," *War on the Rocks*, November 6, 2018, https://warontherocks.com/2018/11/cyber-security-derailed-recommendations-for-smarter-investments-in-infrastructure/.

13 Sean Lyngaas and Kyle Feldscher, "US proposes ban on smart cars with Chinese and Russian tech," CNN.com, September 23, 2024, https://www.cnn.com/2024/09/23/tech/us-car-software-ban-china-russia/index.html.

14 CSIS, "Significant Cyber Incidents," https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

15 David Shepardson, "TikTok CEO: App Has Never Shared US Data with Chinese Government," Reuters, March 21, 2023, https://www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-goverment-2023-03-22/.

16 Rachyl Jones, "Chinese Self-Driving Cars Have Quietly Traveled 1.8 Million Miles on U.S. Roads, Collecting Detailed Data with Cameras and Lasers," *Fortune*, July 8, 2024, https://fortune.com/2024/07/08/chinese-self-driving-cars-us-roads-data-collection-surveillance-national-security-concerns-investigation/.

17 "National Security Law of the People's Republic of China, Article 77," July 1, 2015, DigiChina, Stanford University, https://digichina.stanford.edu/work/national-security-law-of-the-peoples-republic-of-china/.

18 "Cybersecurity Law of the People's Republic of China," June 1, 2017, DigiChina, Stanford University, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

19 See, for instance, Dakota Cary And Kristin Del Rosso, "Sleight Of Hand: How China Weaponizes Software Vulnerabilities," Atlantic Council, September 6, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.

20 "PRC National Intelligence Law," China Law Translate, June 27, 2016, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

21 Rush Doshi, "China's New National Security Laws: Risks to American Companies and Conflicts of Interest," Testimony to the Senate Committee on Homeland Security and Government Affairs, September 24, 2024, 3–4, https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Doshi-2024-09-24.pdf.

22 See, for example, Scott Livingston, "The New Challenge of Communist Corporate Governance," CSIS, January 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210114_Livingston_New_Challenge.pdf. Of course, the United States and most liberal democratic governments also have enacted laws that governments can deploy to compel their companies to cooperate with law enforcement and national security agencies. U.S. law enforcement agencies, for example, can subpoena user information from U.S. technology companies as part of national security and criminal investigations. One 2024 study of disclosures by tech firms, conducted by a company offering VPN (virtual private network) services, found that U.S. authorities—including federal, state, and local law enforcement agencies—had made more than 3.3 million requests for information from tech companies between 2013 and 2022, and that companies generally comply with more than 70 percent of such requests. (See Surfshark, "Report on Government Requests for User Data," August 27, 2024, https://surfshark.com/government-requests-for-user-data.) But Western laws are quite different from China's system: companies can refuse the requests or only comply in the face of subpoenas issued by independent

judges, and requests tend to be limited to individual users or small groups of users, rather than broader categories of information. U.S. companies also are increasingly resisting government requests, or, as Apple and Meta now do, turning on end-to-end encryption services so that they have little information to turn over.

23 Kevin Williams, "CrowdStrike losses May Be Biggest Test Yet of Cybersecurity Insurance Risk Warning from Warren Buffett," CNBC, July 26, 2022, https://www.cnbc.com/2024/07/24/crowdstrike-biggest-test-yet-for-cyber-insurance-buffett-warned-about.html.

24 For a comprehensive survey of Chinese actions to de-risk flows of Chinese data to the United States, see Samm Sacks, Yan Luo, and Graham Webster, "Mapping U.S.–China Data De-Risking: Accumulating Barriers and Safeguards for Data Transfers," DigiChina, Stanford University, February 29, 2024, https://digichina.stanford.edu/wp-content/uploads/2024/03/20240228-dataderisklayout.pdf.

25 See, for instance, U.S.-China Business Council, "Technology Security and IT in China: Benchmarking and Best Practices," July 2016, 1, https://www.uschina.org/sites/default/files/Technology%20Security%20and%20IT%20in%20China%20-%20%20Benchmarking%20and%20Best%20Practices..pdf.

26 Liza Lin, "China Intensifies Push to 'Delete America' from Its Technology," *Wall Street Journal*, March 7, 2024, https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

27 "China's iPhone Ban Accelerates Across Government and State Firms," *Bloomberg*, December 15, 2023, https://www.bloomberg.com/news/articles/2023-12-15/china-s-apple-iphone-ban-accelerates-across-state-firms-government.

28 Peter Hoskins, "China Bans Major Chip Maker Micron from Key Infrastructure Projects," BBC, May 22, 2023, https://www.bbc.com/news/business-65667746; and Ryan McMorrow, Nian Liu, and Qianer Liu, "China Blocks Use of Intel and AMD Chips in Government Computers," *Financial Times*, March 23, 2024, https://www.ft.com/content/7bf0f79b-dea7-49fa-8253-f678d5acd64a.

29 "Tesla Soars on Tentative China Approval for Driving System," *Bloomberg*, April 29, 2024, https://www.bloomberg.com/news/articles/2024-04-29/tesla-clears-key-china-fsd-hurdle-with-baidu-mapping-deal?sref=HblxZSKM.

30 Floris Hulsoff Pul, "EU Drops Sovereignty Rules for U.S. Cloud Providers," *Techzine*, April 4, 2024, https://www.techzine.eu/news/privacy-compliance/118401/eu-drops-sovereignty-rules-for-u-s-cloud-providers/.

31 See John Frittelli, "Shipping Under the Jones Act," R45725 (Washington, DC: Congressional Research Service, November 21, 2019), 2, https://crsreports.congress.gov/product/pdf/R/R45725.

32 Government Accountability Office, "Impact of Changing Foreign Investment and Control Limits on U.S. Airlines," December 1992, 12–13, https://www.gao.gov/assets/rced-93-7.pdf.

33 J. Gregory Sidak, *Foreign Investment in American Telecommunications* (Chicago: University of Chicago Press, (1997), 23–24.

34 Reginald Stuart, "For TV Deal, Murdoch Will Seek U.S. Citizenship," *New York Times*, May 4, 1985, https://www.nytimes.com/1985/05/04/business/for-tv-deal-murdoch-will-seek-citizenship.html.

35 Catherine Belton and Todd C. Frankel, "Sale of Forbes to Group Led by Tech Investor Collapses," *Washington Post*, November 21, 2023, https://www.washingtonpost.com/business/2023/11/21/forbes-sale-russell-musaev/.

36 See Freshfields, "Freshfields Represents Axel Springer on Its Proposed Acquisition of POLITICO," August 26, 2021, https://www.freshfields.com/en-gb/news/2021/08/freshfields-represents-axel-springer-on-its-proposed-acquisition-of-politico/.

37 Federal Communications Commission (FCC), "International Section 214 Application Filing Guidelines," May 14, 2015, https://www.fcc.gov/research-reports/guides/international-section-214-application-filing-guidelines.

38 "FCC Opens Phone Market," CNN, November 25, 1997, https://money.cnn.com/1997/11/25/economy/fcc/.

39 FCC, "Report and Order," November 25, 1997, https://docs.fcc.gov/public/attachments/FCC-97-398A1.pdf.

40 Charles Forelle and Greg Hitt, "U.S. Panel Clears IBM Sale of Unit To Chinese Firm," *Wall Street Journal*, March 10, 2005, https://www.wsj.com/articles/SB111037541128474590. Some government agencies also discontinued their use of Lenovo computers on sensitive networks, although other government agencies continue to procure Lenovo products to this day. Steve Lohr, "State Department Yields on PCs from China," *New York Times,* May 23, 2006, https://www.nytimes.com/2006/05/23/washington/23lenovo.html.

41 George Stahl, "IBM Server Sale to Lenovo Passes U.S. Test," *Wall Street Journal*, August 15, 2014, https://www.wsj.com/articles/ibm-server-sale-to-lenovo-passes-u-s-test-1408135593; Adam Chan, "CFIUS, Team Telecom, and China," *Lawfare*, September 28, 2021, https://www.lawfaremedia.org/article/cfius-team-telecom-and-china; Jay Peters, "Grindr Has Been Sold by Its Chinese Owner after the US Expressed Security Concerns," *The Verge*, March 6, 2020, https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq; Ana Swanson and Paul Mozur, "MoneyGram and Ant Financial Call Off Merger, Citing Regulatory Concerns," *New York Times*, January 2, 2018, https://www.nytimes.com/2018/01/02/business/moneygram-ant-financial-china-cfius.html; and "CFIUS Clearance; Mitigation: China Oceanwide Holdings Group Co. Ltd. and Genworth Financial, Inc.," *The Trade Practitioner*, June 11, 2018, https://www.tradepractitioner.com/2018/06/china-oceanwide-holdings-group-co-ltd-and-genworth-financial-inc/.

42 Todd Shields, "Locke Says Sprint's Chief Was Called About Huawei Bid Concerns," *Bloomberg*, December 7, 2010, https://www.bloomberg.com/news/articles/2010-12-07/commerce-s-locke-says-sprint-s-chief-was-called-about-huawei-bid-concerns?sref=HblxZSKM.

43 Michael Riley, "Obama Invokes Cold-War Law to Unmask Chinese Telecom Spyware," *Bloomberg*, September 30, 2011, https://www.bloomberg.com/news/articles/2011-11-30/obama-invokes-cold-war-security-powers-to-unmask-chinese-telecom-spyware?sref=HblxZSKM.

44 See, for instance, Damian Paletta, Ellen Nakashima, and David J. Lynch, "Trump Administration Cracks Down on Giant Chinese Tech Firm, Escalating Clash with Beijing," *Washington Post*, May 16, 2019, https://www.washingtonpost.com/world/national-security/trump-signs-order-to-protect-us-networks-from-foreign-espionage-a-move-that-appears-to-target-china/2019/05/15/d982ec50-7727-11e9-bd25-c989555e7766_story.html.

45 Katie Rogers and Cecilia Kang, "Biden Revokes and Replaces Trump Order That Banned TikTok," *New York Times*, June 9, 2021, https://www.nytimes.com/2021/06/09/us/politics/biden-tiktok-ban-trump.html.

46 See the Federal Acquisition Supply Chain Security Act of 2018, (Title II of Pub. L. 115-390), signed December 21, 2018.

47 Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain," *Federal Register*, May 15, 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

48 Department of Commerce, "President Trump Declares National Emergency to Secure the Information and Communications Technology Critical Infrastructure Supply Chain," May 15, 2019, https://2017-2021.commerce.gov/news/press-releases/2019/05/president-trump-declares-national-emergency-secure-information-and.html.

49 E.O. 13034, "Protecting Americans Sensitive Data from Foreign Adversaries," *Federal Register*, June 9, 2021, https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries.

50 FCC, "FCC Bans Equipment Authorizations for Chinese Telecommunications and Video Surveillance Equipment Deemed to Pose a Threat to National Security," November 25, 2022, https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat. The FCC also formally banned the use of new Huawei and ZTE communications equipment in the United States.

51 Department of Commerce, "BIS Announces Appointment Of Elizabeth 'Liz' Cannon as Executive Director of Office of Information and Communications Technology And Services," January 22, 2024, https://www.bis.gov/press-release/bis-announces-appointment-elizabeth-liz-cannon-executive-director-office-information.

52 "US Coast Guard Issues Cybersecurity Directive for Chinese-Made Cranes after Biden's Executive Order," *Industrial Cyber*, February 22, 2024, https://industrialcyber.co/regulation-standards-and-compliance/us-coast-guard-issues-cybersecurity-directive-for-chinese-made-cranes-after-bidens-executive-order/.

53 For a summary of E.O. 14117, see Mark Febrizio, "Biden's Ambitious Executive Order Does More for Data Security than Banning TikTok," George Washington University Regulatory Studies Center, April 26, 2024, https://regulatorystudies.columbian.gwu.edu/bidens-ambitious-executive-order-does-more-data-security-banning-tiktok.

54 Sapna Maheshwari and David McCabe, "Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part," *New York Times*, April 23, 2024, https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html.

55 "New Federal Data Broker Law Will Restrict Certain Foreign Data Sales Effective June 23," Wiley, May 7, 2024, https://www.wiley.law/alert-New-Federal-Data-Broker-Law-Will-Restrict-Certain-Foreign-Data-Sales-Effective-June-23. See also Peter Swire, "White Paper on Clarifying Definitions in the Protecting Americans' Data from Foreign Adversaries Act of 2024," Cross Border Data Forum, May 14, 2024, https://www.crossborderdataforum.org/white-paper-on-clarifying-definitions-in-the-protecting-americans-data-from-foreign-adversaries-act-of-2024/.

56 Department of Commerce Bureau of Industry and Security, "Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats," January 14, 2025, https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary.

57 Ana Swanson, "U.S. Weighs Ban on Chinese Drones, Citing National Security Concerns," *New York Times*, January 2, 2025, https://www.nytimes.com/2025/01/02/us/politics/drone-ban-china-security.html.

58 Executive Order, "America First Trade Policy," Sec. 4(d), January 20, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/america-first-trade-policy/.

59 Mike Gallagher and Raja Krishnamoorthi, "Letter to FCC Chair on Chinese Internet Connectivity Modules," August 8, 2023, U.S. House of Representatives Select Committee on the Chinese Communist Party, https://selectcommitteeontheccp.house.gov/media/letters/letter-fcc-chair-chinese-internet-connectivity-modules; John Moolenaar and Raja Krishnamoorthi, "Letter to Commerce on Call for Investigation into Chinese Wi-Fi Routers in U.S. Vulnerable to CCP Hacking & Data Harvesting," U.S. House of Representatives Select Committee on the Chinese Communist Party, August 15, 2024, https://selectcommitteeontheccp.house.gov/media/letters/letter-commerce-call-investigation-chinese-wi-fi-routers-us-vulnerable-ccp-hacking; John Moolenaar and Raja Krishnamoorthi, "Letter to Commerce on Regulation of Foreign Adversary Drones Operating in the U.S.," U.S. House of Representatives Select Committee on the Chinese Communist Party, June 13, 2024, https://selectcommitteeontheccp.house.gov/media/letters/letter-commerce-regulation-foreign-adversary-drones-operating-us;

and Asa Fitch, "Biden Urged to Curb China's Dominance of Older-Generation Chips," *Wall Street Journal*, January 8, 2024, https://www.wsj.com/politics/national-security/lawmakers-push-to-defuse-chinas-dominance-of-older-generation-chips-cbd5adaa.

60 See 15 C.F.R. § 7.4, https://www.ecfr.gov/on/2024-07-17/title-15/subtitle-A/part-7/subpart-A/section-7.4.

61 See Morrison and Forester, "Commerce Issues First-Ever ICTS 'Final Determination' Banning Kaspersky Cybersecurity Products," July 16, 2024, https://www.mofo.com/resources/insights/240716-commerce-issues-first-ever-icts-final-determination.

62 FCC, "List of Equipment and Services Covered By Section 2 of The Secure Networks Act," September 3, 2024, https://www.fcc.gov/supplychain/coveredlist.

63 FCC, "Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act," September 20, 2022, 2n7, https://www.fcc.gov/document/fcc-expands-covered-list-include-china-unicom-and-pacnetcomnet.

64 Department of Commerce, "Proposed Rule: Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," *Federal Register*, January 29, 2024, https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

65 U.S. Department of Justice, "Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable," December 17, 2021, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable.

66 See Peter Swire, "White Paper on Clarifying Definitions in the Protecting Americans' Data from Foreign Adversaries Act of 2024," Cross Border Data Forum, May 14, 2024, https://www.crossborderdataforum.org/white-paper-on-clarifying-definitions-in-the-protecting-americans-data-from-foreign-adversaries-act-of-2024/.

67 E.O. 14083, "Ensuring Robust Consideration Of Evolving National Security Risks By The Committee On Foreign Investment In The United States," *Federal Register*, September 19, 2022, https://public-inspection.federalregister.gov/2022-20450.pdf?1663591529.

68 See H.R. 815, Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, Division H, Protecting Americans from Foreign Adversary Controlled Applications Act, https://www.congress.gov/bill/118th-congress/house-bill/815/text/enr?format=txt&q=%7B%22search%22%3A%22repo+act%22%7D&r=4&s=1

69 Eleanor Olcott, "China's AI Start-Ups Race to Crack US Market," *Financial Times*, October 9, 2024, https://www.ft.com/content/c4acd6f8-f18f-41c7-9d67-b13337df2d0a.

70 Bobby Allyn, "Supreme Court upholds TikTok ban, threatening app's existence in the U.S.," *NPR*, January 17, 2025, https://www.npr.org/2025/01/17/nx-s1-5258396/supreme-court-upholds-tiktok-ban.

71 See Cybersecurity and Infrastructure Security Agency, "Cybersecurity Directives," n.d., https://www.cisa.gov/news-events/directives.

72 Department of Homeland Security, "Issuance of Maritime Security (MARSEC) Directive 105-4; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies," *Federal Register*, February 23, 2024, https://www.federalregister.gov/documents/2024/02/23/2024-03822/issuance-of-maritime-security-marsec-directive-105-4-cyber-risk-management-actions-for-ship-to-shore.

73 *See* Consumer Financial Protection Bureau, "CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies," press release, December 3, 2024, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies/.

74 See, for instance, Cybersecurity and Infrastructure Security Agency, "Cybersecurity Guidance: Chinese-Manufactured UAS," January 17, 2024, https://www.cisa.gov/resources-tools/resources/cybersecurity-guidance-chinese-manufactured-uas.

75 National Counterintelligence and Security Center, "Safeguarding Our Future," June 20, 2023, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

76 Reva Goujon, Jan-Peter Kleinhans and Laura Gormley, "Thin Ice: US Pathways to Regulating China-Sourced Legacy Chips," Rhodium Group, May 13, 2024, https://rhg.com/research/thin-ice-us-pathways-to-regulating-china-sourced-legacy-chips/.

77 Federal Trade Commission, "AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive," February 13, 2024, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive.

78 See, e.g., Surbhi Misra and David Shepardson, "AT&T, Verizon targeted by Salt Typhoon cyberespionage operation, but networks secure," Reuters, December 29, 2024, https://www.reuters.com/technology/cybersecurity/chinese-salt-typhoon-cyberespionage-targets-att-networks-secure-carrier-says-2024-12-29/.

79 Office of Information and Communications Technology and Services, "2024 Technology Prioritization," Bureau of Industry and Security, Department of Commerce, n.d., https://www.bis.gov/media/documents/2024-prioritization-dtd-20240516-1-20240909-revisedpdf.

80 Jill C. Gallagher, "U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests," R47012 (Washington, DC: Congressional Research Service, January 5, 2022), 13, https://crsreports.congress.gov/product/pdf/R/R47012/2.

81 See Jackie Northam, "Government Deadline Approaches To Ban Chinese-Made Surveillance Cameras," NPR, August 8, 2019, https://www.npr.org/2019/08/08/749318323/government-deadline-approaches-to-ban-chinese-made-surveillance-cameras.

82 "FCC votes to bar China's Huawei, ZTE from government subsidy program," Reuters, November 22, 2019, https://www.cnbc.com/2019/11/22/fcc-votes-to-bar-chinas-huawei-zte-from-government-subsidy-program.html.

83 Federal Acquisition Supply Chain Security Act of 2018, (Title II of Pub. L. 115-390), signed December 21, 2018.

84 David E. Sanger, Julian E. Barnes, Raymond Zhong, and Marc Santora, "In 5G Race With China, U.S. Pushes Allies to Fight Huawei," *New York Times*, January 26, 2019, https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html.

85 Executive Order 13873, "Securing the Information and Communications Services Supply Chain," May 15, 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

86 Gallagher, "U.S. Restrictions on Huawei Technologies," 13.

87 Chan, "CFIUS, Team Telecom, and China."

88 Kiran Stacey, "Trump Ban on Chinese Drone Parts Risks Worsening Wildfires," *Financial Times*, August 30, 2020, https://www.ft.com/content/387d2270-eded-4b8d-80e9-b23dd7ff694a.

89 See FCC, "List of Equipment and Services Covered By Section 2 of The Secure Networks Act," September 3, 2024, https://www.fcc.gov/supplychain/coveredlist.

90 Department of Justice, "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States," June 17, 2020, https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

91 Executive Order 13942, "Executive Order on Addressing the Threat Posed by TikTok," August 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/; Executive Order 13943," Executive Order on Addressing the Threat Posed by WeChat," August 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

92 U.S. Department of State, "The Clean Network," n.d., https://2017-2021.state.gov/the-clean-network/.

93 See Ana Swanson, "Trump Bans Alipay and 7 Other Chinese Apps," *New York Times*, January 5, 2021, https://www.nytimes.com/2021/01/05/technology/china-app-ban.html.

94 E.O. 13984, "Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," Trump White House Archives, January 19, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-taking-additional-steps-address-national-emergency-respect-significant-malicious-cyber-enabled-activities/.

95 E.O. 14034, "Protecting Americans' Sensitive Data From Foreign Adversaries," *Federal Register*, June 9, 2021, https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries.

96 41 C.F.R. 201, Federal Acquisition Security Council Rule, August 26, 2021, https://www.federalregister.gov/documents/2021/08/26/2021-17532/federal-acquisition-security-council-rule.

97 Marc S. Martin and Brandon R. Thompson, "FCC Revokes Chinese Telecom's US Authorizations," Perkins Coie, February 4, 2022, https://www.perkinscoie.com/insights/update/fcc-revokes-chinese-telecoms-us-authorizations.

98 Secure Equipment Act of 2021, Pub. L. 117-55, signed November 11, 2021, https://www.congress.gov/bill/117th-congress/house-bill/3919.

99 FCC, "FCC Bans Authorizations for Devices That Pose National Security Threat," November 25, 2022, https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat.

100 Department of Commerce, "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications," *Federal Register*, June 16, 2023, https://www.federalregister.gov/documents/2023/06/16/2023-12925/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.

101 Department of Commerce, "Commerce Department Announces Industrial Base Survey of American Semiconductor Supply Chain," December 21, 2023, https://www.commerce.gov/news/press-releases/2023/12/commerce-department-announces-industrial-base-survey-american.

102 Cybersecurity and Infrastructure Security Agency, "Release Cybersecurity Guidance on Chinese-Manufactured UAS for Critical Infrastructure Owners and Operators," January 17, 2024, https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators.

103 "U.S. Dept. of Commerce proposes new "Know Your Customer" rules for cloud services and AI training," Hogan Lovells, February 26, 2024, https://www.hoganlovells.com/en/publications/us-dept-of-commerce-proposes-new-know-your-customer-rules-for-cloud-services-and-ai-training.

104 White House, "Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports," February 21, 2024, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/.

105 U.S. Commerce Department, "Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles," February 29, 2024, https://www.commerce.gov/news/press-releases/2024/02/citing-national-security-concerns-biden-harris-administration-announces.

106 See U.S. Department of Justice National Security Division, "Data Security," https://www.justice.gov/nsd/data-security.

107 H.R. 815, Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, Division H, Protecting Americans from Foreign Adversary Controlled Applications Act, https://www.congress.gov/bill/118th-congress/house-bill/815/text/enr?format=txt&q=%7B%22search%22%3A%22repo+act%22%7D&r=4&s=1.

108 H.R. 815, Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, Division I, Protecting Americans' Data from Foreign Adversaries Act of 2024, https://www.congress.gov/bill/118th-congress/house-bill/815/text/enr?format=txt&q=%7B%22search%22%3A%22repo+act%22%7D&r=4&s=1.

109 "Commerce Issues Advance Notice of Proposed Rulemaking to Secure Unmanned Aircraft Systems, U.S. Department of Commerce Bureau of Industry and Security," January 2, 2025, https://www.bis.gov/press-release/commerce-issues-advance-notice-proposed-rulemaking-secure-unmanned-aircraft-systems.

Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 170 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Technology and International Affairs Program

The Technology and International Affairs Program develops insights to address the governance challenges and large-scale risks of new technologies. Our experts identify actionable best practices and incentives for industry and government leaders on artificial intelligence, cyber threats, cloud security, countering influence operations, reducing the risk of biotechnologies, and ensuring global digital inclusion.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org