Statement for the Record
of
Jamil N. Jaffer[1]
on
Cyberspace Under Threat in the Era of
Rising Authoritarianism and Global Competition[2]
before the
Subcommittee on East Asia, The Pacific, and
International Cybersecurity Policy
of the
United States Senate Foreign Relations Committee

September 24, 2024

I. Introduction

Chairman Van Hollen, Ranking Member Romney, and Members of the Subcommittee: thank you for inviting me here today to discuss the threats our nation and our allies and partners face in the cyber domain, particularly from authoritarian regimes across the globe that seek to replace the United States as a key international leader.

I want to thank the Chairman and Ranking Member for holding this hearing, given the increasing drumbeat of threats that our nation and other free and open societies face from nations like China,

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and the NSI Cyber & Tech Center and as an Assistant Professor of Law and Director of the National Security Law & Policy Program and the Cyber, Intelligence, and National Security LL.M. Program at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports and invests in innovative companies that develop promising, early-stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers. Mr. Jaffer serves on a variety of public and private boards of directors and advisory boards, including his recent appointment to serve as a member of the Cyber Safety Review Board at the Department of Homeland Security, an advisory board responsible for reviewing and assessing and significant cyber incidents affecting federal civilian and non-federal systems. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer is testifying before this Subcommittee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer or public or private entity. Mr. Jaffer would like to thank Keelin Wolfe, Ann Long, and Patrick Schmidt for their excellent research assistance with respect to this testimony.

[2] Significant portions of this testimony have also been drawn in whole or in part from prior testimony provided by Mr. Jaffer to the Senate Banking Committee in January 2024 and to the House Select Committee on the Chinese Communist Party in September 2024, as well as from an NSI Decision Memo entitled *Addressing the National Security Threat of Chinese Technological Innovation* by Jamil N. Jaffer published in July 2023. Citations to that testimony and paper and quotation marks for portions of this testimony drawn from those materials have been omitted, including where significant portions are excerpted verbatim. Links to both pieces of testimony can be found at the links provided below in footnote 2. In addition, Mr. Jaffer would like to thank Devlin Birnie, Jessica Jones, Harrison McClintock, and Alex Tokie for their excellent research and editing assistance with NSI Decision Memo which can be found at: https://nationalsecurity.gmu.edu/addressing-the-national-security-threat-of-chinese-technological-innovation-2/.

Russia, Iran, and North Korea in the cyber domain. The regimes that control these nations form the core of a growing group of global repressors, nations that repress their own people at home, and then seek to extend that repression abroad, oftentimes not only within their own region but increasingly across the globe as well. Both of you have exhibited strong leadership on the issues at the core of this hearing, including ensuring that America leans forward and leads in the international realm, serving as the strongest ally to our friends and the fiercest foe to our adversaries. As you both well know, the promotion and protection of our national interests, including the protection of our citizens and the critical infrastructure they rely upon could not be more important in this era of expanding authoritarianism and rapidly evolving technologies. It is likewise critically important that, as a global leader, we also defend the democratic principles that undergird free and open societies globally, including the core concepts of free speech, economic liberty, and the rule of law. We must also guard vigilantly against repressive efforts by these regimes as they seek to undermine these democratic principles by depriving their own people and, increasingly, others around the globe, of access to economic freedom and the kind of basic rights that characterize free and open societies.

Chairman Van Hollen, you are well known for your work in this space, including your bipartisan BRINK Act, which requires the imposition of sanctions on the foreign banks and companies that facilitate illegal financial transactions with North Korea, your advocacy to hold the Chinese Communist Party (CCP), which controls the People's Republic of China (PRC) with an iron fist, accountable for its attacks on freedom and democracy in Hong Kong and elsewhere, and your efforts to hold other authoritarian regimes accountable as they seek to expand their repression globally, including by targeting American elections. You also recognize the critical importance of ensuring that American remains competitive and that our critical edge is America's ability to rapidly innovate and that we must protect that innovation with a strong intellectual property system, so thank you for your leadership in those areas as well.

And Ranking Member Romney, you've long been a leading voice on American foreign policy, advocating for policies that promote our economic and national security and that of our allies and partners. You have been one of the primary leaders in our nation—whether during your time as Governor, as a candidate for President, and now in the Senate—that has always been clear-eyed and direct with the American people about the very real threat that we face from nations like Russia, China, Iran, and North Korea. Even when it was unpopular to do so, you have called out these nations for their bad behavior and highlighted the threat they pose to our nation. Whether it was your successful effort to impose a diplomatic boycott during the 2022 Winter Olympics in Beijing or your calling out of Russia from the debate stage over a decade ago—presaging Russia's multiple invasions of Ukraine—no one can doubt where you stand on these issues and the critical importance of your leadership.

Mr. Chairman and Mr. Ranking Member, your bipartisan leadership and continued work together on this Subcommittee is critical to highlighting the many ways that these global repressors have sought to take advantage of our nation's free and open society—particularly in the cyber domain and with respect to emerging technologies—in order to gain political, economic, technological, and military advantage, including in the context of the larger strategic competition taking place across the globe.

And as the members of the Subcommittee know all too well, China is the key economic and national security challenge facing our nation going forward, and its ongoing and expanding collaboration with other global repressors, including in the cyber domain and with respect to emerging technologies, is at the heart of these matters. I hope this hearing will offer us the opportunity to have a candid and frank discussion on these important matters.

I. The Overall Threat Posed by a Rising China and its Collaboration with Other Global Repressors in the Cyber Domain and on Emerging Technologies

As I testified last week before the House Select Committee on the Chinese Communist Party and earlier this year before the Senate Banking Committee, the threat of a rising China, under the leadership of the CCP, is the defining national security challenge facing the United States and our allies today.[3] Like other global repressors, the PRC, under the direction and control of the CCP, is a nation that not only oppresses its own people, but pushes that repression well beyond its borders, not just in the Indo-Pacific region, but across the globe as well. The genocide and crimes against humanity currently underway against Muslim Uyghurs in the Xinjiang region are but one example of the type of repressive activities that take place within the borders of CCP-controlled China, activities that also include the brutal repression of dissent and political, economic, and religious freedom in Hong Kong and Tibet.[4]

[3] *See* Jamil N. Jaffer, *Statement for the Record on How the CCP Uses the Law to Silence Critics and Enforce its Rule*, United States House Select Committee on the Chinese Communist Party (Sept. 19, 2024), *available online at* <https://selectcommitteeontheccp.house.gov/committee-activity/hearings/how-ccp-uses-law-silence-critics-and-enforce-its-rule>; Jamil N. Jaffer, *Statement for the Record on National Security Challenges: Outpacing China in Emerging Technology*, United States Senate Committee on Banking, Housing, and Urban Affairs (Jan. 18, 2024), *available online at* <https://www.banking.senate.gov/imo/media/doc/jaffer_testimony.pdf>.

[4] *See* Michael R. Pompeo, *Press Statement: Determination of the Secretary of State on Atrocities in Xinjiang*, United States Department of State (Jan. 19, 2021), *available online at* <https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/> ("I have determined that since at least March 2017, the…PRC[], under the direction and control of the…CCP[], has committed crimes against humanity against the predominantly Muslim Uyghurs…in Xinjiang….In addition…I have determined that the PRC, under the direction and control of the CCP, has committed genocide against the predominantly Muslim Uyghurs…in Xinjiang."); *see also, e.g.*, United States Department of State, *2021 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)* (Apr. 12, 2022), *available online at* <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/china/>; United States Department of State, *2019 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)* (Mar. 2020), at pp. 89-131 (sections on Tibet and Hong Kong), *available online at* < https://www.state.gov/wp-content/uploads/2020/03/CHINA-INCLUSIVE-2019-HUMAN-RIGHTS-REPORT.pdf>.

The global scale of the CCP's repression is vast, as can be seen in the PRC's near-constant drumbeat of military and economic threats against Taiwan,[5] its hostile actions and active threats towards other U.S. allies and partners globally,[6] its export of surveillance technologies and other repressive capabilities to authoritarian-leaning regimes worldwide,[7] its ongoing efforts to consolidate control over and withhold access to key critical minerals and strategic metals,[8] its extortion of dozens of countries under the Belt and Road Initiative (BRI),[9] and its growing political, economic, and military relationships with other global repressors like Russia, Iran, and North Korea.[10]

But this litany of activities is only the beginning of the CCP's larger and more hidden effort to undermine our nation's security. The CCP has also long engaged in the broad-based theft of intellectual property from American and allied private sector companies to benefit its own economic base,[11] and the PRC's deep and expanding cyber infiltration of U.S. and allied critical infrastructure,[12] as well as its active installation of capabilities to hold such critical infrastructure at risk,[13] together pose a clear and present danger to our economic and national security. Likewise, the CCP has actively sought to recruit American and allied academics and intellectuals through its Thousand Talents Program[14] and has sought to shape minds of students through its establishment of hundreds of Confucius Institutes across the globe.[15]

For the purposes of today's hearing, I'd like to focus on three area where the CCP seeks in particular to undermine U.S. interests in the cyber and emerging technologies domain: (1) the effort by China to embed its technologies around the globe in an effort to collect intelligence and influence political, economic, and military conditions; (2) the way the CCP is likely to exploit emerging technologies, like artificial intelligence, steal intellectual property, and use extortive efforts to undermine U.S. and allied leadership globally; and (3) the CCP's holding at risk of American and allied critical infrastructure in the cyber domain and to influence American and allied views. And I'd also like to highlight how China and other global repressors, like Russia, use international institutions, like the U.N. and various advisory committees and boards to also achieve their own ends. Finally, I'd like to focus on how we might usefully address some of these issues.

---

[5] *See, e.g.*, Nectar Gan, et al., *China Starts "Punishment" Military Drills Around Taiwan Days After Island Swears in New Leader*, CNN (May 23, 2024), *available online at* <https://edition.cnn.com/2024/05/22/asia/china-military-drills-taiwan-punishment-intl-hnk/index.html>.

[6] *See, e.g.*, Matthew Olay, *Threat From China Increasing, Air Force Official Says*, DOD News (Sept. 16, 2024) *available online at* <https://www.defense.gov/News/News-Stories/Article/Article/3907669/threat-from-china-increasing-air-force-official-says/> ("[T]he Chinese Communist Party continues to heavily invest in capabilities, operational concepts and organizations that are specifically designed to defeat the United States and its allies' ability to project power…including weapons targeting U.S. land and sea assets like air bases and aircraft carriers."); Agnes Chang, et al., *China's Risky Power Play in the South China Sea*, N.Y. Times (Sept. 15, 2024), *available online at* <https://www.nytimes.com/interactive/2024/09/15/world/asia/south-china-sea-philippines.html>.

[7] *See, e.g.*, Bulelani Jili, *China's Surveillance Ecosystem and the Global Spread of its Tools*, Issue Brief, Atlantic Council (Oct. 17, 2022), *available online at* <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/>; Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports*, Brookings Inst. (Apr. 2024), *available online at* <https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf>.

[8] *See, e.g.*, Jared Cohen, et al., *Resource Realism: The Geopolitics of Critical Mineral Supply Chains*, Goldman Sachs Global Institute (Sept. 13, 2023), *available online at* <https://www.goldmansachs.com/insights/articles/resource-realism-the-geopolitics-of-critical-mineral-supply-chains> ("China now accounts for 85 – 90% of global REEs mine-to-metal refining…Likewise, China refines 68% of the world's cobalt, 65% of nickel, and 60% of lithium of the grade needed for electric vehicle batteries…Even though new discoveries of critical mineral reserves around the world continue to be made, China is still the top producer of 30 of the 50 critical minerals, in part because it mines at greater rates than other countries."); *see id*. ("In 2010, Beijing embargoed REE exports to Tokyo…[i]n 2020, China reportedly cut off exports of graphite to Sweden. Following up on the October 2022 US-led export controls on advanced computing and semiconductor products…Beijing announced its own export controls on gallium and germanium products to the United States in the summer of 2023.").

[9] *See, e.g.*, Jamil N. Jaffer, *Waking up to the Threat of the Chinese Communist Party: A Call to Action from Congress*, The Hill (Feb. 28, 2023) (op-ed), available online at <https://thehill.com/opinion/national-security/3877095-waking-up-to-the-threat-of-the-chinese-communist-party-a-call-to-action-from-congress/> (arguing that "the CCP's Belt and Road Initiative, while masquerading as an economic development program, is actually a tool for massive economic theft and political coercion, designed to supply the Chinese government with resources and jobs for its population, while addicting developing nations to Chinese financing that they can't possibly repay"); *see also* Reid Standish, *A Closer Look At China's Controversial Lending Practices Around The World*, Radio Free Europe/Radio Liberty (Apr. 22, 2021), *available online at* <https://www.rferl.org/a/china-loans-around-the-world/31217468.html>; Anna Gelpern, et al., *How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments*, AidData, et al. (Mar. 2021) at 5-9, 34-45, *available online at* <https://www.cgdev.org/sites/default/files/how-china-lends-rare-look-100-debt-contracts-foreign-governments.pdf>.

[10] *See, e.g.*, Max Bergmann, et al., *Collaboration for a Price: Russian Military-Technical Cooperation with China, Iran, and North Korea*, Center for Strategic International Studies (May 22, 2024), *available online at* <https://www.csis.org/analysis/collaboration-price-russian-military-technical-cooperation-china-iran-and-north-korea>; *see also, e.g.*, Kimberly Donovan & Maia Nikoladze, *The Axis of Evasion": Behind China's Oil Trade with Iran and Russia*, The Atlantic Council (Mar. 28, 2024), *available online at* <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-axis-of-evasion-behind-chinas-oil-trade-with-iran-and-russia/>.

[11] *See, e.g.*, Jamil N. Jaffer, *Addressing the National Security Threat of Chinese Technological Innovation*, National Security Institute (Aug. 2023), at 1, *available online at* <https://nationalsecurity.gmu.edu/wp-content/uploads/2023/08/The-National-Security-Threat-of-Chinese-Technological-Innovation.pdf> ("Over time, the PRC came to rely upon the theft of U.S. intellectual property at industrial scale—referred to as the greatest transfer of wealth in modern human history—to create an entire industry of state-owned and state-influenced enterprises that, when combined today, generate a tremendous amount of the technology products and capabilities sold around the globe.") (internal citations omitted); Senator Carl Levin, *Opening Statement of Chairman Carl Levin in Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program*, Senate Armed Services Committee (Mar. 27, 2012), at 3, *available online at* < https://www.armed-services.senate.gov/imo/media/doc/12-19%20-%203-27-12.pdf> ("General Alexander has stated that the relentless industrial espionage being waged against U.S. industry and Government chiefly by China constitute 'the largest transfer of wealth in history.'").

[12] *See* Cybersecurity and Infrastructure Security Agency, et al., *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Alert Code: AA24-038A (Feb. 7. 2024), *available online at* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

[13] *See id*.; *see also* text accompanying n. 58 *infra*.

[14] *See, e.g.*, Alison Snyder, *China Talent Program Increased Young Scientists' Productivity, Study Says*, Axios (Jan. 10, 2023), *available online at* <https://www. axios.com/2023/01/10/china-funding-young-scientists-productivity> (describing the Youth Thousand Talents Program (YTT), which offers more than 3,500 young researchers—both Chinese nationals and foreign-born scientists—funding and benefits to relocate full-time to China and also describing the Thousand Talents Program, a large effort that began in 2008 with the goal of recruiting top-caliber scientists to work with China; a part of that effort often allowed or even encouraged recruits to remain at their U.S. institutions while also working with the PRC); *see also* Emily S. Weinstein, *Chinese Talent Program Tracker*,

II. China's Effort to Embed its Technologies Around the Globe in an Effort to Collect Intelligence and Influence Political, Economic, and Military Conditions.

China's ongoing and widespread effort to embed its technologies around the globe can be seen in numerous places across the globe. For example, the effort to embed Huawei and ZTE gear in the telecommunications networks of Western countries, including successful efforts in a number of U.S. states as well as at the heart of the British Telecom and other allied networks, and has been well-understood for over a decade.[16] Indeed, as far back as March 2015, as part of its Belt-and-Road Initiative, China announced a Digital Silk Road effort—ostensibly to provide aid to other nations to improve their telecom networks, AI capabilities, cloud computing, and surveillance technology, among other things—that puts Chinese national champions, like Huawei, deep in those networks.[17] Capabilities like these—which provide direct access into the core of the telecommunications networks—can be hugely valuable to our adversaries as a tool to collect massive amounts of information and intelligence, as well as to conduct actual offensive cyber attacks that can delete, destroy, or modify information and even take down entire networks.[18] Yet

---

Center for Security and Emerging Technology, Georgetown University (Nov. 2020), *available online at* <https://cset.georgetown.edu/publication/chinese-talent-program- tracker/> (noting that Chinese talent initiatives include 43 national-level programs and 200 talent programs at sub-national levels, numbers that are growing as the PRC "seeks to retain, manage, and recruit talent globally"); Federal Bureau of Investigation, *The China Threat - Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage*, Federal Bureau of Investigation, *available online at* <https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese- talent-plans> (describing hundreds of talent programs that incentivize their members to "steal foreign technologies needed to advance China's national, military, and economic goals" including work on key programs like military technologies, nuclear energy, wind tunnel design, and advanced lasers, and noting that talent plan participants "enter into a contract with a Chinese university or company—often affiliated with the Chinese government—that usually requires them to [be] subject [] to Chinese laws, to share new technology developments or breakthroughs...[and to] recruit other experts into the program").

[15] Thomas Lum & Hannah Fischer, *Confucius Institutes in the United States: Selected Issues*, Congressional Research Service (May 2, 2023), *available online at* <https://crsreports.congress.gov/product/pdf/IF/IF11180>.

[16] *See* Chairman Mike Rogers & Ranking Member C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, House Permanent Select Committee on Intelligence, U.S. House of Representatives (Oct. 8, 2012), *available online at* <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf>; *see also* Andy Keiser & Bryan Smith, *Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat*, National Security Institute (Jan. 24, 2019), *available online at* <https://nationalsecurity.gmu.edu/chinese-telecommunications/>.

[17] *See* Joshua Kurlantzick, *Assessing China's Digital Silk Road Initiative*, Council on Foreign Relations (Dec. 18, 2020), *available online at* <https://www.cfr.org/ china-digital-silk-road/>; Chang Che and John Liu, *'De-Americanize': How China Is Remaking Its Chip Business*, New York Times (May 11, 2023), *available online at* <https://www. nytimes.com/2023/05/11/technology/china-us-chip-controls.html>.

[18] *See* Rogers & Ruppersberger, *Huawei and ZTE Investigative Report*, *supra* n. 16 at 3 ("The ability to deny service or disrupt global systems allows a foreign entity the opportunity to exert pressure or control over critical infrastructure on which the country is dependent. The capacity to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that advances China's economic place in the world. Access to U.S. telecommunications infrastructure also allows China to engage in undetected espionage against the United States government and private sector interests….Inserting malicious hardware or software implants into Chinese-manufactured telecommunications components and systems headed for U.S. customers could allow Beijing to shut down or degrade critical national

many nation-states have taken a while to understand the very real threat these capabilities pose to their national security and some continue to install these systems at the heart of their networks.[19] Indeed, according to one source, as of two years ago, "Huawei and its components comprise almost 70% of the total 4G networks across the [African] continent."[20]

Likewise, Congress and two successive Administrations have highlighted the very real threat that social media applications, like TikTok, pose to our national security.[21] This national security threat is described in extensive detail in an amicus brief that was filed on my behalf and that of well over a dozen other former U.S. government national security officials—including two former U.S. Attorneys General and a former U.S. National Cyber Director—in litigation brought by TikTok in the United States Court of Appeals for the District of Columbia Circuit.[22] That brief, which supported the U.S. government's position defending legislation signed into law earlier this year, is attached as an appendix to this testimony. The brief argues, in relevant part, that TikTok's extensive collection on data on Americans and our allies, its close ties to the CCP and the PRC government, and the CCP's influence over TikTok's algorithm, which has previously pushed pro-Chinese and anti-American content as well as actively suppressed anti-CCP content, means that TikTok, "presents a serious and unique national security threat to the United States."[23]

And while many Americans view TikTok as a tool for kid's dance videos and short-form entertainment, the sad reality is that over the course of the last decade, this Chinese-government influenced tool has become the primary source of news for Americans under the age of 30,[24] a fact that should deeply trouble all of us. Even more concerning, given the massive amount of data that TikTok collects on its users, when combined with other data stolen by Chinese government hackers targeting the U.S. federal government, including the security clearance files thousands of current and former U.S. government officials holding Top Secret-Sensitive Compartmented Information (TS/SCI) clearances, and private companies holding sensitive financial, health, and travel data of millions of Americans, it is clear that TikTok's data—when fed into modern artificial intelligence algorithms—can help drive future sophisticated intelligence collection and disinformation

---

security systems in a time of crisis or war. Malicious implants in the components of critical infrastructure, such as power grids or financial networks, would also be a tremendous weapon in China's arsenal.").

[19] *See, e.g.*, Michael Nienaber, *Germany to Cut Huawei From 5G Core Network by End-2026*, BNN Bloomberg (July 11, 2024), *available online at* <https://www.bnnbloomberg.ca/business/company-news/2024/07/10/germany-agrees-to-strip-huawei-from-5g-core-network-by-end-2026/>.

[20] *See, e.g.*, Arjun Gargeyas, *China's '2035 Standards' Quest to Dominate Global Standard-Setting*, Hinrich Foundation (Feb. 21, 2023), *available online at* <https://www.hinrichfoundation.com/research/article/trade-and-geopolitics/china-2035-standards-project-restructure-global-economy/>

[21] *See, e.g.*, *Protecting Americans from Foreign Adversary Controlled Applications Act*, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024); The White House, *Protecting Americans' Sensitive Data from Foreign Adversaries*, 86 Fed. Reg. 31423 (June 9, 2021); The White House, *Addressing the Threat Posed by TikTok*, 85 Fed. Reg. 48637-38 (Aug. 6, 2020).

[22] *See* Brief of Former National Security Officials, *TikTok Inc. and ByteDance Ltd. v. Merrick B. Garland*, No. 24-1113 (consolidated with others), Document #2067987 (filed Aug. 2, 2024) (attached hereto as Exhibit A).

[23] *Id*. at 1-7, 11-14.

[24] *Id*. at 10-11.

campaigns targeting American citizens and our allies.[25] Indeed, the Office of the Director of National Intelligence (ONDI) recently indicated that "China is demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI," and noted that "TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties during the U.S. midterm election cycle in 2022."[26]

III. China's Exploitation of Emerging Technologies, Theft of Intellectual Property, and Use of Extortive Efforts to Undermine U.S. and Allied Leadership Globally

Likewise, at the core of the national security threat that the PRC poses to the United States, as well as our global competition with China for supremacy—whether in the economic, political, military, or social spheres—is technological innovation, including access to and control over critical emerging technologies, particularly in the artificial intelligence domain.[27] In recent decades, the PRC has made aggressive moves to build its own technological innovation base and now seeks to expand those capabilities.[28] Much of this effort by the PRC initially began by actively seeking to dominate the manufacturing market for technology goods, producing equipment at costs well below those achievable in most other economies.[29] This was achieved, in significant part, by

---

[25] *Id*. at 3-10.

[26] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024), at 12, *available online at* <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.

[27] *See, e.g.*, The White House, National Security Strategy (Oct. 2022), at 23, *available online at* <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden- Harris-Administrations-National-Security-Strategy-10.2022.pdf> ("The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it…It is using its technological capacity and increasing influence over international institutions to create more permissive conditions for its own authoritarian model, and to mold global technology use and norms to privilege its interests and values."); Xi Jingping, *Speech to Members of the Chinese Academy of Sciences, the Chinese Academy of Engineering, and the National Congress of China Association for Science and Technology* (May 28, 2021) (translated by Zichen Wang), *available online at* <https://www.pekingnology.com/p/xi-jinpings-speech-on- science-and?s=r> ("[S]cientific and technological innovation has become the main battlefield of the international strategic game, and the competition around the commanding heights of science and technology is unprecedentedly fierce.").

[28] *See, e.g.*, Tarun Chhabra, et. al, *Executive Summary – Global China: Assessing China's Growing Role in the World, Brookings Institution* (Apr. 2020), *available online at* <https://www.brookings.edu/articles/global-china-technology/> ("China's rapid technological advances are playing a leading role in contemporary geopolitical competition….While the U.S. has maintained its position as the technologically dominant power for decades, China has made enormous investments and implemented policies that have contributed significantly to its economic growth, military capability, and global influence. In some areas, China has eclipsed, or is on the verge of eclipsing, the United States — particularly in the rapid deployment of certain technologies."); Bloomberg News, *How China Aims to Counter US 'Containment' Efforts in Tech*, Washington Post (Mar. 30, 2023), available online at <https://www.washingtonpost.com/business/2023/03/30/explainer-how-china-aims-to-counter-us-containment-efforts-in-tech/cea71f0c-cf1d-11ed-8907-156f0390d081_story.html> ("Chinese President Xi Jinping…and his new lieutenants are deploying what they call a "whole nation" system: marshaling resources and companies from across the country — and trillions of dollars — to drive research and development.").

[29] *See* Wayne M. Morrison, *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*, Congressional Research Service (June 25, 2019), at 23, *available online at* <https://crsreports.congress.gov/product/pdf/RL/RL33534> ("China's abundance of low-cost labor has made it internationally competitive in many low-cost, labor-intensive manufactures. As a result, manufactured products constitute a significant share of China's trade. A substantial amount of China's imports is comprised of parts and

exploiting the PRC's theft of U.S. intellectual property at industrial scale—referred to as the greatest transfer of wealth in modern human history[30]—which was then leveraged to create an entire industry of state-owned and state-influenced enterprises that, when combined today, generate a tremendous amount of the technology products and capabilities sold around the globe, including producing goods on behalf of a number of highly innovative American companies, competing with others, and replacing or coopting yet others in the global market.[31] Worse still, the PRC is now going well beyond manufacturing-at-scale and is creating innovation on top of this stolen IP and securing its access to data, as it recognizes that whichever nation dominates the technology revolution—particularly in emerging technology areas like quantum computing, biotechnology, and artificial intelligence (the latter of which is particularly data reliant)—will likely also win the larger geopolitical competition.[32]

A key aspect of the PRC's effort to lead in the technology domain is its centralized planning efforts that have been in place for well over a decade, including its Made in China 2025 line of effort ("PRC 2025"), a "broad set of industrial plans that aim to boost competitiveness by advancing China's position in the global manufacturing value chain, 'leapfrogging' into emerging technologies, and reducing reliance on foreign firms."[33] This effort aims to enable China to "make major technology breakthroughs, lead innovation in specific industries, and set global standards" by 2035 and "[l]ead global manufacturing and innovation with a competitive position in advanced technology and industrial systems" by 2049, with key areas of focus including next generation IT and telecommunications capabilities, high performance computing, advanced robotics, and artificial intelligence.[34] And in the critically important AI domain, China released a plan back in 2017—long before the public advent of highly-capable generative AI in 2022 and even well prior to the enactment of the U.S. National AI Initiative Act of 2020—to "lead the world in AI by 2030."[35] While ostensibly emphasizing domestic development in these national plans, it is clear that the PRC plans to continue to rely on the "acquisition, absorption, and adaptation of foreign technology by PRC entities that recast these capabilities as their own,"[36] and then build upon these stolen technologies to create additional innovation.

---

components that are assembled into finished products, such as consumer electronic products and computers, and then exported.")

[30] *See* Jaffer, *Addressing the National Security Threat*, *supra* at n. 11.

[31] *See, e.g.*, Special Competitive Studies Project, *Generative AI: The Future of Innovation Power* (Oct. 2023), at 3 & n.6 (collecting sources), 10-12 and 23, *available online at* <https://www.scsp.ai/wp-content/uploads/2023/10/economy.pdf>; Brady Helwig, et al., *National Action Plan for Advanced Compute & Microelectronics*, Special Competitive Studies Project (Nov. 2023), at 8-9, 13, 32, and 39, *available online at* <https://www.scsp.ai/wp-content/uploads/2023/11/National-Action-Plan-for-U.S.-Advantage-in-Advanced-Compute-and-Microelectronics.pdf>; *see also, e.g.*, John Miller & Sacha Wunsch-Vincent, *High-Tech Trade Rebounded Strongly in the Second Half of 2020, with New Asian Exporters Benefiting* (Mar. 15, 2021), *available online at* <https://www.wipo.int/pressroom/en/news/2021/news_0001.html>.

[32] *Id.*

[33] *See* Karen M. Sutter, "Made in China 2025" Industrial Policies: Issues for Congress, Congressional Research Service (Mar. 10, 2023), at 1, available online at <https://crsreports.congress.gov/product/pdf/IF/IF10964>.

[34] *Id.*

[35] *See* SCSP, *Generative AI*, *supra* at n. 31, at 3 & n. 6.

[36] *Id.*

And in February of this year, the Director of National Intelligence released her Annual Threat Assessment, which she describes China's efforts to "become a world [science & technology] superpower and to use this technological superiority for economic, political, and military gain."[37] According to ODNI, "Beijing is trying to fast-track its S&T development through investments, intellectual property (IP) acquisition and theft, cyber operations, talent recruitment, scientific and academic collaboration, and illicit procurements," and noted specifically that "[i]n 2023, a key PRC state-owned enterprise has signaled its intention to channel at least $13.7 billion into emerging industries such as AI, advanced semiconductors, biotechnology, and new materials."[38]

As noted above, China's acquisition of U.S. and allied emerging technology takes place through a range of vectors: (1) outright theft of intellectual property;[39] (2) forced technology transfer from companies seeking to enter the Chinese market;[40] (3) requiring new market entrants to establish joint ventures with PRC companies;[41] (4) requiring sensitive IP to be kept in China;[42] (5) tax incentives to get production and R&D moved to China;[43] (6) acquisition of American and allied companies with sensitive technologies directly or through bankruptcy proceedings;[44] (7) corporate and government partnerships with U.S. companies, universities, and individual experts or academics, including through PRC talent programs and educational pipeline work;[45] and (8)

---

[37] *See* ODNI, *Annual Threat Assessment*, *supra* n. 26 at 9.

[38] *Id*.

[39] *See, e.g.*, Office of the U.S. Trade Representative, *2023 Special 301 Report*, Executive Office of the President, The White House (Apr. 2023), at 9, 22-23, 45-47, *available online at* <https://ustr.gov/sites/default/files/2023-04/2023Special301Report.pdf>; *see also* Keith B. Alexander and Jamil N. Jaffer, *China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around*, Barron's (August 4, 2020), *available online at* <https://www.barrons.com/ articles/china-is-waging-cyber-enabled-economic-war-on-the-u-s-how-to-fight-back-51596587400>.

[40] *Id*.

[41] *See, e.g.*, Sean O'Connor, *How Chinese Companies Facilitate Technology Transfer from the United States*, U.S.-China Economic Security Review Commission, at 7 (May 6, 2019), *available online at* <https://www.uscc.gov/sites/default/files/Research/HowChineseCompaniesFacilitateTechTransferfromtheUS.pdf>

[42] *Id*. at 8.

[43] *See, e.g.*, Erica York, et al., *Comparing the Corporate Tax System in the U.S. & China*, Tax Foundation, at 4 (May 2022), *available online at* <https://files.taxfoundation.org/20220502152914/Comparing-the-Corporate-Tax-Systems-in-the-United-States-and-China.pdf>.

[44] See, e.g., Cory Bennet & Bryan Bender, *How China Acquires 'The Crown Jewels' of U.S. Technology*, Politico (May 22, 2018), available online at <https://www. politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413>; Camille A. Stewart, *Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings*, 10 J. Nat'l Security L. & Pol'y 277, 279-82 (2019).

[45] *See, e.g.*, Alison Snyder, *China Talent Program Increased Young Scientists' Productivity, Study Says*, Axios (Jan. 10, 2023), *available online at* <https://www. axios.com/2023/01/10/china-funding-young-scientists-productivity>; *see also* Emily S. Weinstein, *Chinese Talent Program Tracker*, Center for Security and Emerging Technology, Georgetown University (Nov. 2020), *available online at* <https://cset.georgetown.edu/publication/chinese-talent-program- tracker/>; Federal Bureau of Investigation, *The China Threat - Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage*, Federal Bureau of Investigation, available online at <https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese- talent-plans>.

joining and setting the agenda for international standards setting bodies.[46] And China has doubled down on these efforts, making clear that it will continue to exploit its foreign research connections, use domestic regulatory measures and influence abroad in areas like antitrust, IP, and international standards,[47] as well as make massive investments into key emerging technology areas, including quantum computing, robotics, artificial intelligence, and cybersecurity,[48] both directly and by offering low-interest and no-interest loans and massive state-driven subsidies—totaling well-over a trillion dollars—to enable its companies to compete more favorably in global markets,[49] while also using board seats to influence corporate decision-making.[50]

We know also that China continues to build out its STEM workforce, proactively recruiting leading STEM players from around the world,[51] and, having already passed the U.S. in the number of annual Ph.Ds awarded many years back, some estimate that the PRC may annually graduate nearly double the number of STEM Ph.Ds as the U.S. in the near future.[52] All of these efforts are also buttressed by China's longer-term efforts to secure its access to critical minerals, strategic metals, and energy resources, from production to processing,[53] and its parallel efforts to exclude U.S. and

---

[46] *See* Gargeyas, *China's '2035 Standards' supra* n. 20.

[47] See Sutter, *Made in China 2025*, *supra* n. 33 at 2 ("Similarly, the FYP calls for an expanded use of antitrust, IP, and standards tools—in China and extraterritorially—to set market terms and promote the export of MIC2025 goods and services now coming to market. The FYP also emphasizes the value of China's foreign research ties in developing China's own competencies in a range of MIC2025 technology areas.").

[48] *See id.*

[49] *See, e.g.*, Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests*, Congressional Research Service (Jan. 5, 2022), at 7-8, *available online at* <https://crsreports.congress.gov/product/pdf/R/R47012/2> (describing how "[n]ational champions [in China], including Huawei, received preferential policy treatment, access to low-cost financing, R&D funding, and tax benefits"); *see also, e.g.*, Ann Harrison, et al., *Can a Tiger Change Its Stripes? Reform of Chinese State-Owned Enterprises in the Penumbra of the State*, NBER Working Paper No. 25475 (Jan. 2019), at 24, *available online at* <https://www.nber.org/system/files/working_papers/w25475/w25475.pdf> (noting that former Chinese state-owned enterprises, like SOEs themselves, generally "retain ready access to large loans, concessionary interest rates, and outright subsidies").

[50] *See, e.g.*, Scott Livingston, *The New Challenge of Communist Corporate Governance*, Center for Strategic & International Studies (Jan. 2021), at 2-4, *available online at* <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210114_Livingston_New_Challenge.pdf>.

[51] *See, e.g.*, Eric Schmidt, *To Compete With China on Tech, America Needs to Fix Its Immigration System*, Foreign Affairs (May 16, 2023), *available online at* <https://www.foreignaffairs.com/united-states/eric-schmidt-compete-china-tech-america-needs-fix-its-immigration-system> ("While the United States' dysfunctional system increasingly deters the world's top scientists, researchers, and entrepreneurs, other countries are proactively recruiting them. China is particularly active in doing so, with direction coming from the very top.").

[52] *See, e.g.*, Karin Fischer, *China Outpaces U.S. in STEM*, Georgetown Center for Security and Emerging Technology, Latitudes (Aug. 9, 2021), *available online at* <https://cset.georgetown.edu/article/china-outpaces-u-s-in-stem/>. ("China could graduate nearly twice as many STEM PhDs as the United States by 2025…China overtook the U.S. in PhD production in 2007 and has steadily increased its lead ever since.").

[53] *See* Jane Nakano, *The Geopolitics of Critical Minerals Supply Chains*, Center for Strategic & International Studies, at 5 (March 2021), *available online at* <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210311_Nakano_Critical_Minerals.pdf>.

allied partners from access to such resources, all of which are critical to our technological and industrial innovation base.[54]

IV. China's Effort to Hold American and Allied Critical Infrastructure at Risk and Influence American and Allied Views

According to ODNI, "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."[55] ODNI noted that "PRC operations discovered by the U.S. private sector probably were intended to pre-position cyber attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia" and it assesses that "[i]f Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets…[in] a strike [that] would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces."[56]

And just a few days earlier, the FBI Director had gone perhaps further saying, "[t]here has been far too little public focus on the fact that PRC hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American….China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities."[57] Providing a bit more detail on the targeting of American infrastructure, the FBI Director explained that the FBI and "our partners identified hundreds of routers that had been taken over by the PRC state-sponsored hacking group known as Volt Typhoon," which contained "malware [that] enabled China to hide, among other things, pre-operational reconnaissance and network exploitation against critical infrastructure like our communications, energy, transportation, and water sectors." According to the FBI Director, these efforts represented "[s]teps China was taking…to find and prepare to destroy or degrade the civilian critical infrastructure that keeps us safe and prosperous…represent[ing] real-world threats to our physical safety."[58]

---

[54] *See, e.g.*, Arjun Kharpal, *What are Gallium and Germanium? China Curbs Exports of Metals Critical to Chips and Other Tech*, *CNBC* (July 4, 2023), *available online at* <https://www.cnbc.com/2023/07/04/what-are-gallium-and-germanium-china-curbs-exports-of-metals-for-tech.html>; *see also* Mai Nguyen, *China's Rare Earths Dominance in Focus After it Limits Germanium & Gallium Export*s, Reuters (July 5, 2023), *available online at* <https://www.reuters.com/markets/commodities/ chinas-rare-earths-dominance-focus-after-mineral-export-curbs-2023-07-05/>.

[55] *See* ODNI, *Annual Threat Assessment*, *supra* n. 26 at 12

[56] *Id.*

[57] *See* Christopher A. Wray, *Director Wray's Opening Statement*, House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Jan 31, 2024), *available online at* <https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party>.

[58] *Id.*

And the Cybersecurity and Infrastructure Security Agency (CISA), in a document jointly released by CISA, FBI, NSA, and a number of other federal and foreign intelligence agencies from Australia and New Zealand, indicated that this new posture—installing capabilities that could have a clear potential disruptive effect—said, "Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions."[59]

And just a few days ago, the FBI announced that it had taken down a widespread Chinese botnet, associated with a threat actor named Flax Typhoon which had infected over a quarter-million devices across North America, South America, Europe, Africa, Southeast Asia and Australia with malware.[60] This botnet, which was ostensibly focused on espionage, not disruption, nonetheless demonstrated the scale and access of Chinese hacking, with over half the devices, made up of "home routers, firewalls, storage devices, and Internet of Things devices like cameras and video recorders," being located in the U.S. And, perhaps more troublingly, the FBI noted that the Flax Typhoon actors "shared some of the infrastructure for its attacks" with the Volt Typhoon actors.[61]

Moreover, it's not just hacking or disruptive attacks that are in play; we also increasingly see the CCP actively taking a page out of the Russian covert influence playbook by seeking to, in the words of ODNI, "sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence."[62] According to ODNI, "Beijing's information operations primarily focus on promoting pro-China narratives, refuting U.S.-promoted narratives, and countering U.S. and other countries' policies that threaten Beijing's interests, including China's international image, access to markets, and technological expertise" and that it is now also seeking to "actively exploit perceived U.S. societal divisions using its online personas" and "mold U.S. public discourse—particularly on core sovereignty issues, such as Hong Kong, Taiwan, Tibet, and Xinjiang," while also potentially seeking to "influence the U.S. elections in 2024 at some level because of its desire to sideline critics of China and magnify U.S. societal divisions."[63]

All of these efforts demonstrate a commitment on the part of the CCP to get significantly more aggressive in the cyber domain, even as we recall that back in 2019, ODNI assessed that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the

[59] *See* CISA, et al., *PRC State-Sponsored Actors Compromise and Maintain Persistent Access*, *supra* n. 12.

[60] *See* Sam Sabin, Chinese Hacking "Typhoons" Threaten U.S. Infrastructure, Axios (Sept. 20, 2024), available online at <https://www.axios.com/2024/09/20/china-critical-infrastructure-cyberattacks>.

[61] *Id.*

[62] *See* ODNI, *Annual Threat Assessment*, *supra* n. 26 at 12.

[63] *Id.*

United States" and that Russia could do much of the same with respect to electrical distribution networks, while Iran could also do much the same to a large company's corporate network.[64]

V. China and Russia's Efforts to Use the International System to Achieve Their Goals

Finally, it may also be worth noting the efforts of China and Russia to use the international system, including the U.N. and various international standards setting bodies to achieve their own goals. China, for its part, has engaged in an effort to obtain additional influence in global organizations technical standard-setting bodies "by increasing the number of Chinese officials, technocrats, and private sector leaders for key leadership positions in major working groups and technical committees of international technical standard-setting bodies"[65] which it reportedly has used to "push[] for the acceptance of Chinese businesses' standards as the de facto international technical standards in several crucial sectors," and its "'Standards 2035' project also aims for the country to go global with its technical standards, especially by strategically employing its high-level officials and leaders of domestic technology enterprises at the organizations responsible for determining global technical standards."[66] And more recently, according ODNI, "China also announced [an] Global AI Governance Initiative to bolster international support for its vision of AI governance."[67]

Russia and China also recently got a significant win in the international realm with respect to a major cyber policy initiative, the U.N. Convention Against Cybercrime, with the Russian-led text—with some compromise language, to be fair—being adopted by consensus action of the Ad-Hoc Committee on Cybercrime last month.[68] For years, the United States pushed back against the Russian-proposed language and process, which it historically viewed as being overly aggressive and subject to manipulation and abuse by authoritarian regimes.[69] While the U.S. supported certain provisions of the treaty as being an appropriate exercise of law enforcement authority for nation-sates, as at larger level, the U.S. did not support the treaty because it lacked the type of rule-of-law safeguards that American laws typically contain.[70] More recently, however, the U.S. backed off this position and allowed the Ad-Hoc Committee to push the Russian-led language out by consensus.[71] As the convention heads to the General Assembly for approval and, if approved, ratification by just over three dozen countries for entry into force, there has been a significant backlash from both industry and non-governmental organizations, and there is some possibility

---

[64] *See* ODNI, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Jan. 29, 2019), *available online at* <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

[65] *See* Gargeyas, *China's '2035 Standards' Quest*, *supra* n. 20.

[66] *Id*.

[67] *See* ODNI, *Annual Threat Assessment*, *supra* n. 26 at 9.

[68] *See* Agence France Presse, *UN Approves its First Treaty Targeting Cybercrime*, Barron's (Aug. 8. 2024), *available online at* <https://www.barrons.com/news/un-approves-its-first-treaty-targeting-cybercrime-93801d31>.

[69] *See* Jason Pielemeier, *Rethinking the United Nations Cybercrime Treaty*, Just Security (Sept. 23, 2024), *available online at* <https://www.justsecurity.org/100333/rethinking-united-nations-cybercrime-treaty/>.

[70] *See* AFP, *UN Approves First Treaty*, *supra* n. 68.

[71] *See* Pielemeier, *Rethinking the UN Cybercrime Treaty*, *supra* n. 69.

that the convention may get further delayed or halted, particularly if the United States returns to its prior position of objecting to the convention writ large.[72]

VI. Potential Responses to Consider in Addressing the Threats Posed By Global Repressors in the Cyber and Emerging Technologies Domains

Given all this, one might ask what ought be done to address these very real challenges. Below are a few initial thoughts.

1. **Provide Appropriations for Basic Science Research and Workforce Development**. The U.S. government has long been one of the key seed funders of critical basic science research in American universities and industry, and this has led to major breakthroughs in areas where countries like China now seek to compete including in biotechnology, high-performance computing, quantum computing, and artificial intelligence.[73] Ensuring that some of the key provisions in the CHIPS and Science Act and other such legislation, including funding for next generation communications technologies and artificial intelligence, continues to be provided is critical.[74]

2. **Avoid Taking Action that Would Limit Private Sector R&D Spending and Instead Incentivize It in Critical Areas**. Today, the private sector represents 70% of all R&D expenditures in the United States, with technology companies leading the way, making up

---

[72] *Id.*

[73] *See* James Manyika et al., *Innovation and National Security - Keeping Our Edge*, Council on Foreign Relations (Sep. 2019), at 2, 19, *available online at* <https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf> ("Federally supported R&D had a dramatic impact on U.S. competitiveness and national security. According to a 2019 study, starting in the 2010s nearly one-third of patented U.S. inventions relied on federally funded science []. Touch screens, the Global Positioning System (GPS), and internet technologies central to the smartphone are all products of Defense Department research...Between 1988 and 2010, $3.8 billion of federal investment in genomic research generated an economic impact of $796 billion and created 310,000 jobs. A new wave of support for basic research could have similar economic and military benefits."); *see also* Jamie Gaida et al., *ASPI's Critical Technology Tracker: The Global Race for Future Power*, Australian Strategic Policy Institute (Feb. 2023), at 1, *available online at* <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/ASPIs%20Critical%20 Technology%20Tracker_0.pdf> (noting that "China's global lead extends to 37 out of 44 technologies that ASPI is now tracking, covering a range of crucial technology fields spanning defence, space, robotics, energy, the environment, biotechnology, artificial intelligence (AI), advanced materials and key quantum technology areas").

[74] *See, e.g.*, Pub. L. No. 117-167, §§ 10101-114 (basic science); §§ 10221-235 (basic science); §§ 10311-321 (STEM education & workforce) & §§ 10501-526 (STEM education & workforce); *see also* Madeline Ngo, *CHIPS Act Funding for Science and Research Falls Short*, New York Times (May 30, 2023), *available online at* <https://www.nytimes. com/2023/05/30/us/politics/chips-act-science-funding.html> ("The total funding for research agencies was nearly $3 billion short of authorized levels this year, according to a recent Brookings Institution analysis...[T]he director of the National Science Foundation[] said the money would help the nation lead in industries that were listed as key focus areas in the law, such as artificial intelligence and biotechnology....[and] could also help the agency expand A.I. research and training programs aimed at building up the nation's STEM work force, which agency officials said were critical since the country is facing a shortage of workers to build semiconductors."); *see also* Matt Hourihan, *Analysis: As Congress Considers COMPETES, How Short Are We From The Old COMPETES?*, American Association for the Advancement of Science (Feb. 22, 2022), *available online at* <https://www.aaas.org/sites/default/files/2022-02/AAAS%20COMPETES%20Shortfalls%20Feb%20 2022_0.pdf> .

seven of the top ten R&D spenders, including all of the top five.[75] Core R&D spending, along with our permissive economic and legal environment and the availability of significant amounts of venture and growth capital, as well as a highly- skilled workforce, is what makes America the technology innovation hub of the globe. These capabilities are not only at the heart of our economic success, they are also a core reason why our national defense capabilities remain relatively unmatched across the globe today. If we are to compete effectively with the PRC, we need to incentivize, not limit the capabilities of the top R&D investors in the U.S., including the technology companies that are in the top five R&D spenders in the nation. To do so, we must avoid the temptation to artificially restrain successful innovators in the absence of actual, demonstrable bad behavior, while also providing new tax and other economic incentives for increased private R&D investment—both for new entrants as well as existing players that can scale—in a range of areas like high-performance computing, quantum technology, AI/ML, trust, safety, and security, and the design and production, in the United States and allied nations, of leading-edge semiconductor capabilities.

3. **Incentivize Technology Infrastructure Investment**. For the better part of the last six decades, the United States has benefited significantly from being the core hub of the global telecommunications infrastructure. As the place where much of the world's telecommunications systems come together, particularly when it comes to global Internet traffic, the United States has been able to innovate rapidly and gain both economic and national security benefits from this convergence.[76] t is critical that the government provide the right incentivizes for industry to build out both domestic and allied computing and communications infrastructure and invest in the capacity and innovation to deliver such capabilities globally while also continuing efforts to rip and replace adversary gear, whether it is in state, local or allied systems. To that end, the government should provide tax and other economic incentives for increased private investment in the development of such technologies, the broader deployment of large-scale computing infrastructure to support cloud and edge computing, the replacement of adversary technology, and the expansion of AI capabilities being made available to U.S. and allied innovators.

4. **Maintain U.S. Capacity for Innovation.** Ensuring that the United States is able to access the underlying manufacturing capacity and workforce necessary to support a modern

---

[75] *See* Jamil N. Jaffer, *NSI Backgrounder: The Role of American Technology Sector in Safeguarding U.S. Economic and National Security*, National Security Institute, GMU Scalia Law School (Dec. 2022), at 1 & n. 6, *available online at* <https://nationalsecurity.gmu.edu/the-role-of-american-technology-sector-in- safeguarding-u-s-economic-and-national-security/> (citing John F. Sargent, *U.S. Research and Development Funding and Performance: Fact Sheet*, Congressional Research Service (Sept. 13, 2022), *available online at* <https://crsreports.congress.gov/product/pdf/R/R44307/18>); *see id*. at 1 & n. 5 (citing Prableen Bajpai, *Which Companies Spend the Most in Research and Development (R&D)?*, Nasdaq (June 21, 2021), *available online at* <https://www.nasdaq.com/articles/which-compa- nies-spend-the-most-in-research-and-development-rd-2021-06-21>).

[76] *Cf.* Manyika et al., *Innovation and National Security*, *supra* n. 73 at 2, 19, *available online at* <https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf> ("This seventy-year strength arose from the expansion of economic opportunities at home through substantial investments in education and infrastructure, unmatched innovation and talent ecosystems, and the opportunities and competition created by the opening of new markets and the global expansion of trade. ").

technology and communications infrastructure—including consistent access to semiconductors, critical minerals, and other core materials necessary to support major technological innovation—will also be of strategic importance to the United States in the coming years. It is critical that government and industry work together to create the right tax and regulatory incentives to ensure that American and allied companies invest their money here (and in allied nations) to create much-needed capacity and to ensure that we have the skilled workers necessary to build and maintain this capacity.

5. **Avoid Harmful Overregulation.** To ensure that the United States remains a leader in technology innovation, it is critical that the United States avoid adopting significant new regulatory or administrative policies that would undermine the ability of the United States to effectively compete on a global scale. Efforts in recent years to amend longstanding and highly effective antitrust laws that have served our economy well for decades,[77] are a key example of the kind of new policies that would be highly detrimental in the context of the ongoing economic and national security competition with China. These efforts, which target a handful of technology companies based on the nature and scale of their business, are largely driven by policy issues unrelated to innovation or competition.[78] As such, they would likely undermine the very companies that have the largest potential to benefit the United States and our allies by posing the biggest threat to the PRC's effort to win the technology competition and sends exactly the wrong message to new entrants: namely, that if small, innovative businesses thrive and become highly successful, expanding not through unfair competition, but through market success, the government might seek to target them for special attention, creating laws to cut them down to size.[79] To the extent there are concerns that market power actually is being used to undermine competition, existing

[77] *See, e.g.*, American Innovation and Choice Online Act, S.2992, 117th Cong. (2021); Open App Markets Act, S.2710, 117th Cong. (2021).

[78] Bill Evanina & Jamil N. Jaffer, *Kneecapping U.S. Tech Companies Is a Recipe for Economic Disaster*, Barron's (June 17, 2022), *available online at* <https://www.barrons.com/articles/kneecapping-u-s-tech-firms-is-a-recipe-for-economic-disaster-51655480902> ("Conservatives are often worried—sometimes for good reason—that certain social or mainstream media companies might actively seek to suppress or quiet conservative voices. On the liberal side, there are a range of legitimate concerns with technology companies, including the displacement of traditional labor in the new gig economy... Yet rather than tackling these concerns directly by going after the specific behaviors or actions that trouble ordinary Americans, politicians in Washington have chosen instead to vilify some of our most successful companies and to go after them economically."); *see also* David R. Henderson, *A Populist Attack On Big Tech*, The Hoover Institution (Mar. 3, 2022), *available online at* <https://www. hoover.org/research/populist-attack-big-tech-0>.

[79] Klon Kitchen & Jamil Jaffer, *The American Innovation & Choice Online Act Is A Mistake*, The Kitchen Sync (Jan. 19, 2022), *available online at* <https://www. thekitchensync.tech/p/the-american-innovation-and-choice> ("Going after our technology companies, particularly a targeted shot at certain big ones, sends the wrong message to startups and investors alike; it tells them that if you are innovative enough to be successful and grow significantly larger, you may be targeted for different treatment....This undermines not only the companies that are likely to be investing in R&D over the next decade and generating some of the key innovations that will contribute to our national security, it also undermines a central proposition that has created a robust tech ecosystem in this country: take risk, innovate, fail fast and often, and when you succeed, reap the rewards so long as you don't exploit your position to gain unfair advantage."); Evanina & Jaffer, *Kneecapping U.S. Tech Companies*, *supra* n. 78 ("Picking and choosing individual companies to be treated differently than others under our antitrust laws is inconsistent with the heart of our economic system, which Seeks to reward innovation and success, not penalize them.").

law—and the longstanding consumer welfare standard that undergirds them—when used appropriately, can effectively address these concerns.[80]

6. **Avoid Being Tempted By the European Model.** There are those who argue that the U.S. ought enact laws like the General Data Protection Regulations, the Digital Markets Act, the Digital Services Act, and the AI Act in order to make sure we are keeping up on the latest in regulatory creep.[81] The reality, however, if one looks at the economic and innovation scoreboard as between the United States and Europe—when looking at GDP growth, the creation of highly successful, highly innovative businesses, or building private companies whose technology innovations have a massive benefit for national and economic security—it tilts decisively in favor of the U.S. today, as it has for the last five decades at least.[82] Unlike Europe, which often seeks to drive specific market outcomes, the United States has generally sought to institute a broadly applicable set of rules designed to ensure that all market participants compete fairly. Sticking with the traditional American approach is the right way to go.

7. **Incentivize AI and Emerging Technology Innovation and Focusing Any Regulation Only on Critical Gaps**. The approach that best protects U.S. national and economic security in AI and emerging technology is one that allows innovation to flourish, stepping cautiously to address legitimate concerns where regulation is warranted and appropriate, based on traditional considerations like a demonstrable market failure. Rather than rushing to broad-based regulation, as the European Parliament has recently, the wiser approach, consistent with the American approach to innovation, would be to identify potential regulatory need, assesses whether regulation is necessary and appropriate, and prioritize the voluntary adoption of industry-driven frameworks, before moving to a regulatory posture, which in turn would build upon the voluntary frameworks.[83] While much has been written about the potential of AI to cause significant harm, the fact is that AI has the potential to have a transformative effect on human society, raising all boats and allowing a broad range of workers to do mundane tasks more efficiently while freeing innovators to create even more productive tools and capabilities.[84] As such, the best approach on AI may

[80] *See* Henderson, *A Populist Attack on Big Tech*, *supra* n. 78; Evanina & Jaffer, *Kneecapping U.S. Tech Companies*, *supra* n. 78.

[81] *See, e.g.*, Cecilia Kang, *As Europe Approves New Tech Laws, the U.S. Falls Further Behind*, New York Times (April 22, 2022), *available online at* <https://www. nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html>

[82] *See* Jan Rybnicek, *Innovation in the United States and Europe*, in *Report on the Digital Economy*, Global Antitrust Institute (2020), available online at <https://gaidigitalreport.com/2020/08/25/innovation-in-the-united-states-and-europe/>; Michael Ringel et al., *The Most Innovative Companies 2020, The Serial Innovation Imperative*, Boston Consulting Group, at 16 (June 2020), *available online at* <https://web-assets.bcg.com/img-src/BCG-Most-Innovative-Companies-2020-Jun-2020-R-4_tcm9-251007.pdf>; *see also* Loren Thompson, *Why Reining In Big Tech Could Be Bad News For U.S. National Security*, Forbes (July 7, 2022), *available online at* <https://www.forbes.com/sites/lorenthompson/2022/07/07/why-breaking-up-big-tech-could-be-bad-news-for-us-national-security/?sh=1e40190d32bd>; Jaffer, *The Role of American Technology Sector*, *supra* n. 75.

[83] *Cf. Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards & Technology (Apr. 16, 2018), *available online at* <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

[84] *Compare* Geoffrey Hinton, et al., *Statement on AI Risk: AI Experts and Public Figures Express their Concern About AI Risk*, Center for AI Risk (May 30, 2023), *available online at* <https://www.safe.ai/statement-on-ai-

be the more cautious one: encouraging those closest to the actual creation of the technology to craft potential frameworks and industry best practices that might guide the trusted, safe, and secure development and implementation of these technologies.

8. **Stop Investing in Our Adversaries.** In 2022, the total U.S. foreign direct investment in China was $126.1 billion, an increase of more than $10 billion from the prior year.[85] American companies have made major investments in leading-edge Chinese companies, including in the artificial intelligence arena, and by one metric, U.S. investors "accounted for nearly a fifth of investment deals in Chinese AI/ML companies from 2015 to 2021."[86] We must take sustainable action to limit on outbound investment from the U.S. in critical industries like high performance computing, semiconductors, critical minerals, cloud computing, artificial intelligence, and quantum computing, to name just a few.

9. **Growing a STEM-Capable Workforce By Investing Here and Fixing Our Broken Immigration System.** The U.S. must take action to grow our STEM workforce, including continuing appropriate funding the workforce-related programs authorized in the CHIPS and Science Act and directing new and existing resources to the states in form of block grants to be used through public schools, public charter schools, and private institutions.[87] We must also incentivize those who come from abroad to study here to stay here, develop their new technology, and build businesses in the United States, rather than forcing them to back home. One of the nation's most enduring achievements is our "ability to attract and retain some of the world's best STEM talent...[that can] drive research and development efforts," yet our current immigration system makes little sense, because it allows a wide range of undergraduate and graduate students to benefit from our world-class

---

risk#open-letter> ("Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.") *with* Michael Chui, et al., *Generative AI is Here: How Tools Like ChatGPT Could Change Your Business*, McKinsey & Co. (Dec. 20, 2022), *available online*

at <https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business>; Danny Hajek, et al., *What Is AI and How Will It Change Our Lives?*, NPR (May 25, 2023), *available online at* <https://www.npr.org/2023/05/25/1177700852/ai- future-dangers-benefits>.

[85] *See* Bureau of Economic Analysis, *Direct Investment by Country and Industry, 2022*, U.S. Dept. of Commerce (July 20, 2023), *available online at* <https://www. bea.gov/sites/default/files/2023-07/dici0723.pdf>.

[86] *See* Emily S. Weinstein & Ngor Luong, *U.S. Outbound Investment into Chinese AI Companies*, Georgetown University Center for Security & Emerging Technology (Feb. 2023), at 11-13, available online at <https://cset.georgetown.edu/wp-content/uploads/CSET-U.S.-Outbound-Investment-into-Chinese-AI-Companies.pdf> *see also* Alexandra Alper, *U.S. Investors Have Plowed Billions into China's AI sector, Report Shows*, Reuters (Feb. 1, 2023), *available online at* <https://www.reuters.com/ technology/us-investors-have-plowed-billions-into-chinas-ai-sector-report-shows-2023-02-01/>.

[87] *See* McKinsey & Co., *The CHIPS and Science Act: Here's What's in It* (Oct. 4, 2022), *available online at* <https://www.mckinsey.com/industries/public-sector/ our-insights/the-chips-and-science-act-heres-whats-in-it>; *cf.* National Science Teachers Association, *FACT SHEET: Title IV, Part A of ESSA: Student Support and Academic Enrichment Grants and Science/STEM Education*, *available online at* <https://static.nsta.org/pdfs/ESSATitleIV-ScienceSTEMFactSheet.pdf> (describing the $1.65 billion Student Support and Academic Enrichment block grant program under The Every Student Succeeds Act (ESSA) enacted in 2014, which consolidated the Math and Science Partnership Grants, which is described as "the largest single program at the Department of Education devoted exclusively to science/STEM-related classroom purposes," having "received $152.7M in FY2016 before it was eliminated").

higher education system, but then—with exception of the small number that are able to obtain H-1B visas or otherwise stay in the United States—requires them to return home to build businesses abroad.[88] This poorly thought-out policy actually forces American companies to hire high-skilled workers abroad and deprives our own economy of the benefits of their employment here, including the tax revenues and spending of these high-skilled, high-wage workers who could easily be vetted to address any potential IP theft and foreign intelligence concerns.[89]

10. **Set a Clear, Declaratory Cyber Deterrence Policy and Where Needed Take Action to Deter Future Attacks.** If we are to take seriously the threat posed by China and other nations that are actively targeting our critical infrastructure, we cannot simply remain on the defensive; rather, we must implement effective deterrence in the cyber domain. We can do so being clear about what kind of activity we can tolerate and what kind of activity would cross a line; we must talk about our offensive capabilities in the cyber domain to demonstrate one way we might effectuate that deterrence; and, having established a clear line, we must be willing to enforce it and impose significant consequences on bad actors and we must do so in a way that is open and transparent so we are able to deter both the current and future actors.[90] While there are those that argue such a policy is too provocative or more likely to get us into a conflict, the reality is that we are already in state of sustained low-level combat in the cyber domain, and that it has gotten worse in recent years not better.[91] The fact of the matter is that when our adversaries don't know how we might react—or worse, based on prior practices assume that we won't react all—they are more likely to push the envelope and test our boundaries.[92]

VII. Conclusion

For over a decade now, Congress and the Executive Branch have been talking the very real threats that globally repressive nations like China, Russia, Iran, and North Korea pose to the United States,

---

[88] *See* William Alan Reinsch & Thibault Denamiel, *Immigration Policy's Role in Bolstering the U.S. Technology Edge*, Center for Strategic & International Studs. (Feb. 6, 2023), *available online at* <https://www.csis.org/analysis/immigration-policys-role-bolstering-us-technology-edge>; *see also* Gina M. Raimondo, *Remarks by U.S. Sec'y of Com. Gina Raimondo on the U.S. Competitiveness and the China Challenge*, U.S. Department of Commerce (Nov. 20, 2022), *available online at* <https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china>; *see also* Eric Schmidt, *To Compete With China on Tech, America Needs to Fix Its Immigration System*, Foreign Affairs (May 16, 2023), *available online at* <https://www.foreignaffairs.com/united-states/eric-schmidt-compete-china-tech-america-needs-fix-its-immigration-system>.

[89] *See* Paayal Zaveri, *America's Immigration System is a Nightmare & it's Forcing Tech Companies to Move Jobs Outside of the Country*, Business Insider (Mar. 14, 2023), *available online at* <https://www.businessinsider.com/us-tech-firms-offshoring-immigration-labor-shortage-issues-remote-work-2023-3>.

[90] *See* Jamil N. Jaffer, *Statement for the Record*, Safeguarding the Federal Software Supply Chain, Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability

(Nov. 29, 2023), *available online at* <https://oversight.house.gov/wp-content/uploads/2023/11/Written-Statement-Jaffer.pdf>.

[91] *Id.*

[92] *Id.*

particularly in the cyber domain and with respect to emerging technologies. And while we have taken significant action to address some of these threats, the reality is that we are far from where we need to be if we are going to successfully limit the threat these nations pose. It is critical that the United States take swift action, alongside our allies, to limit the threats we face in the cyber domain and to limit our exposure to the threats that are apparent in the emerging technology domain as well while continuing to lead on innovation. To do any less would be significant mistake.

EXHIBIT
A

ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024

No. 24-1113, 24-1130, 24-1183

UNITED STATES COURT OF APPEALS
FOR THE D.C. CIRCUIT

TIKTOK INC. AND BYTEDANCE LTD.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

consolidated with

caption continued on inside cover

On Petitions for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act

BRIEF OF AMICI CURIAE FORMER NATIONAL SECURITY OFFICIALS

Thomas R. McCarthy
Kathleen S. Lane
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com
katie@consovoymccarthy.com

August 2, 2024

Counsel for Amici Curiae

BRIAN FIREBAUGH, CHLOE JOY SEXTON, TALIA CADET, TIMOTHY MARTIN, KIERA SPANN, PAUL TRAN, CHRISTOPHER TOWNSEND, and STEVEN KING

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

BASED POLITICS INC.

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rules 26.1 and 28(a)(1) and Fed. R. App. 26.1 the undersigned counsel certifies as follows:

A. Parties and Amici

The parties to *TikTok Inc. v. Garland*, No. 24-1113, are Petitioners TikTok Inc and ByteDance Ltd., and Respondent Merrick B. Garland, in his official capacity as Attorney General of the United States. The parties to the first consolidated case, *Firebaugh v. Garland*, No. 24-1130, are the Creator Petitioners and Respondent Garland, in his official capacity as Attorney General of the United States. The parties to the second consolidated case, *BASED Politics Inc. v. Garland*, No. 24-1183, are Petitioner BASED Politics Inc. and Respondent Garland, in his official capacity as Attorney General of the United States. As of the finalization of this brief, the following amici have either filed a brief or a notice of intent to participate: Electronic Frontier Foundation, Freedom of the Press Foundation, TechFreedom, Media Law Resource Center, Center for Democracy and Technology, First Amendment Coalition, Freedom to Read Foundation, The Cato Institute, Professor Matthew Steilen, Arizona Asian American Native Hawaiian and Pacific Islander for Equity Coalition, Asian

American Federation, Asian Americans Advancing Justice Southern California, Calos Coalition, Hispanic Heritage Foundation, Muslim Public Affairs Council, Native Realities, OCA-Asian Pacific American Advocates of Greater Seattle, South Asian Legal Defense Fund; Sikh Coalition, Sadhana, San Francisco, Knight First Amendment Institute at Columbia University, Free Press, Pen American Center, Milton Mueller, Timothy H. Edgar, Susan A. Aaronson, Hans Klein, Hungry Panda US, Inc., Shubhangi Agarwalla, Enrique Armijo, Derek Bambauer, Jane Bambauer, Elettra Bietti, Ashutoh Bhagwat, Stuart N. Brotman, Anupam Chander, Erwin Chemerinsky, James Grimmelmann, Nikolas Guggenberger, G.S. Hans, Robert A. Heverly, Michael Karanicolas, Kate Klonick, Mark Lemley, David S. Levine, Yvette Joy Liebesman, Dylan K. Moses, Sean O'Brien, Christopher J. Sprigman.

Because these petitions were filed directly in this Court, there were no district court proceedings in any of the cases.

B. Rulings Under Review

The petitions seek direct review of the constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act

(H.R. 815, Div. H, 118th Cong., Pub. L. No. 118-50 (April 24, 2024). There were no district court proceedings in any of the cases.

C. Related Cases

Amici are not aware of any other case pending before this or any other court that is related.

Dated: August 2, 2024

/s/ Thomas R. McCarthy
Thomas R. McCarthy

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Executive Branch Sources

Congressional Sources

News Sources

Other Authorities

GLOSSARY

Act	Protecting Americans from Foreign Adversary Controlled Applications Act
CCP	Chinese Communist Party
DNI	Director of National Intelligence
FBI	Federal Bureau of Investigation
OMB	Office of Management and Budget
OPM	Office of Personnel Management

INTEREST OF AMICI CURIAE

Amici curiae are former national security government officials in their individual capacities.[1] Amici are filing this brief to address the national security concerns surrounding TikTok, ByteDance, and those entities' ties to a foreign adversary—the Chinese Communist Party.

Amici have served at the highest levels of government, in national security, intelligence, and foreign policy roles. They have served under different administrations, for leaders of different political parties, during different global conflicts, and have different foreign policy concerns. Despite their differences, amici have all served with a common goal and purpose: securing this Nation and protecting it from foreign threats. TikTok presents one such critical foreign threat. As former government officials and as national security experts, amici have a strong interest in ensuring that the Court understands and appreciates the national security interests at stake in this litigation. Amici are identified in Appendix A.

[1] No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund its preparation or submission. No person other than the amici or their counsel made a monetary contribution to the preparation or submission of this brief.

SUMMARY OF ARGUMENT

Approximately 170 million Americans use TikTok. Like other social media applications, TikTok collects massive amounts of personal data on its users, and TikTok has a proprietary algorithm that curates what each user sees on the app. Unlike other social media applications, however, TikTok is subject to the direction and control of the Chinese Communist Party. Congress, recognizing the national security threat posed by CCP control over TikTok sought to address this threat by enacting the Protecting Americans from Foreign Adversary Controlled Applications Act.

TikTok is owned by a Chinese company beholden to the Chinese Communist Party. Chinese government control over TikTok affords the CCP direct access to the massive amounts of personal data of those 170 million American TikTok users, and it allows the CCP to manipulate what those Americans see and share on TikTok. The former enables the CCP to collect, use, and exploit those vast swaths of personal information for its own benefit. As FBI Director Wray put it, TikTok is "one of the most valuable surveillance tools on the planet." *Hearing on the 2023 Annual Threat Assessment of the U.S. Intelligence Community* at 1:09:00, U.S. Senate Select Comm. Intelligence Hearing (Mar. 8, 2023) (testimony

of Director Wray) ("*2023 Threat Assessment Hearing*"), https://perma.cc/3YJG-XQDJ. And the latter enables the CCP to deploy TikTok as a widescale propaganda and misinformation machine to influence American policy debates. Indeed, TikTok sent its 170 million American users a prompt mischaracterizing the Act's divestment requirement as a flat ban on TikTok and encouraging them to call their representatives in Congress to oppose the Act. Sapna Maheshwari & David McCabe, *TikTok Prompts Users to call Congress to Fight Possible Ban*, N.Y. Times (Mar. 7, 2024), https://perma.cc/GD3J-QNPV.

Amici agree with the United States that the Act is a lawful exercise of Congressional authority to protect national security and that it does not run afoul of the First Amendment or any other Constitutional proscription. Amici write separately to underscore the grave national-security threats posed by Chinese control of TikTok; to highlight TikTok's failure to take any meaningful action to reduce those threats; and to explain that the compelling national security interests behind the Act overcome any applicable level of First Amendment scrutiny.

ARGUMENT

I. The Chinese government's control of TikTok presents a novel and serious national security threat.

TikTok presents a serious and unique national security threat to the United States because the data it collects is made available to the Chinese Communist Party and its ability to influence information shared through the application is subject to the direction and control of the CCP. TikTok collects massive amounts of information about the 170 million Americans using its application. USA.Br. 1, 18-39; *House lawmakers deeply concerned over TikTok despite CEO's testimony*, CBS News (Mar. 23, 2023), https://perma.cc/H95J-PETG. TikTok acknowledges that it automatically collects, among other things, its users profile information and image; connections between individual users; content shared between users; private messages; information found in a device's clipboard; and purchase and payment information. *Privacy Policy*, TikTok (last updated July 1, 2024), https://perma.cc/RV8S-U38H. Along with this information, TikTok collects voice and location data, and, perhaps most troublingly, the application may listent to users even when they are not using the application and even when their privacy settings are set to prohibit such collection. *The Select: 'TikTok Special'-A weekly Committee Recap* (Mar.

8, 2024), https://perma.cc/Z7YH-SW9S. In the aggregate, this vast dataset provides significant and deep insights into those using TikTok's application.

What makes TikTok unique from other social-media applications is that the CCP has direct access to this vast dataset. TikTok is owned by ByteDance, a Chinese corporation that is "beholden to the CCP." *Hearing on 2024 Annual Threat Assessment* at 1:09:50, U.S. Senate Select Committee Intelligence Hearing (Mar. 11, 2024) (statement of Director Wray), https://perma.cc/5ZMS-ZVR4; *see also Annual Threat Assessment of the U.S. Intelligence Community*, DNI Office (Feb. 5, 2024), https://perma.cc/NLG3-Z6R7. And China's National Intelligence Law requires ByteDance and TikTok to assist with intelligence gathering. *Letter from Rep. Mike Gallagher to Christopher Wray, FBI Director*, at 1 (Dec. 7, 2023), https://perma.cc/R352-UFKG. This means that ByteDance must provide China's intelligence agencies with direct access to the extensive personal data TikTok collects on its more than 170 million American users. *See Safeguarding Our Future*, The National Counterintelligence and Security Center, https://perma.cc/549G-W4X2; *see also* USA.Br. 17.

Beyond the access the CCP has to the data of American citizens, it is well-documented that the CCP also has significant *internal* influence over TikTok. The CCP requires certain companies, like TikTok, to host an internal party committee, which has the "sole function" of ensuring "compliance with [CCP] orthodoxy." *See Hearing on Oversight of the Federal Bureau of Investigation* at 3:19:00, House Judiciary Committee (July 12, 2023) (statement of Director Wray), https://perma.cc/87HV-YR8D; *see also* Kevin Breuninger & Eamon Javers, *Communist Party cells influencing U.S. companies' China operations*, CNBC (July 12, 2023), https://perma.cc/TU6B-GHYV. In some cases, the company's charter directly incorporates these internal party committees, giving the CCP even more power over "management decisions" and ensuring that CCP personnel "serve in management or board positions." Scott Livingston, *The New Challenge of Communist Corporate Governance*, Ctr. for Strategic & Int'l Studies (Jan. 2021), https://perma.cc/X3KY-AYLC; *see also* Lauren Yu-Hsin Lin & Curtis J. Milhaupt, *CCP Influence over China's Corporate Governance*, Stanford Ctr. on China's Economy and Institutions (updated Nov. 1, 2022), https://perma.cc/PYL3-DDN2.

Taken together, this means that TikTok automatically collects substantial amounts of data on over 170 million Americans, which is then directly accessible by the CCP—whether through Chinese intelligence laws or through internal pressure and control from those planted within the company to carry out CCP's policy objectives. Indeed, a former TikTok executive confirmed that CCP members were specifically stationed at ByteDance in order to review data collected through TikTok, and to influence internal decisions about how the TikTok algorithm works to convey information to its users, including more than 170 million Americans. *See* Zen Soo, *Former ByteDance executive says Chinese Communist Party tracked Hong Kong protesters via data*, AP News (June 7, 2023), https://perma.cc/K9HB-XDBL; Thomas Fuller & Sapna Maheshwari, *Ex-ByteDance Executive Accuses Company of 'Lawlessness,'* N.Y. Times (May 12, 2023), perma.cc/DE96-KD7G. The pressure the CCP exerts on TikTok and its parent, ByteDance, is also readily apparent. For example, last year, ByteDance executives publicly apologized for deviating from "socialist core values" for "vulgar" content on one of its other applications. *See* Yaqiu Wang, *The Problem with TikTok's Claim of Independence from Beijing*, The Hill (Mar. 24, 2023), https://perma.cc/L44R-U9HL. And

ByteDance has used its data collection to track political activity, including activities of Hong Kong protestors and commentary by American journalists. *See* Emily Baker-White, *EXCLUSIVE: TikTok Spied on Forbes Journalists*, Forbes (Dec. 22, 2022), https://perma.cc/XUS8-ATNP; Soo, *supra*; *TikTok: How Congress Can Safeguard American Data Privacy*, Hearing Before the H. Comm. on Energy & Commerce, 118th Cong. (2023) ("*2023 House Data Privacy Hearing*"). The CCP's control over TikTok and its direct access to the personal data of 170 million Americans standing alone therefore presents grave national security concerns.

These concerns are only heightened by the fact that the Chinese government has access to massive amounts of additional highly sensitive data—data belonging to hundreds of millions of Americans that China has obtained through cyber operations undertaken by sophisticated Chinese-government intelligence and military hackers. *See, e.g.*, *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions*, Dep't of Justice (May 9, 2019) ("*Anthem Breach*"), https://perma.cc/77P4-T7Y5; *Chinese Military Hackers Charged in Equifax Breach*, Federal Bureau of Investigation (Feb. 10, 2020) ("*Equifax Breach*"), https://perma.cc/7JPH-G2EC; David E. Sanger, et al.,

Marriott Data Breach is Traced to Chinese Hackers, N.Y. Times (Dec. 11, 2018), https://perma.cc/3EJT-BPL9; *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, Dep't of Justice (Feb. 10, 2020), https://perma.cc/9GRX-QR4V. In the OPM breach, hackers working on behalf of the Chinese government exfiltrated over 20 million personnel records of American government employees holding Top Secret/Sensitive Compartmented Information (TS/SCI) clearances, collecting social security numbers, dates and places of birth, addresses, and detailed background check data—including "financial data; information about spouses, children and past romantic relationships; and any meetings with foreigners"—on the very government employees that the U.S. government entrusts with its most sensitive classified intelligence information. *See* Sanger, *supra*. Through the Anthem hack, the Chinese government also obtained the addresses, birth dates, and social security numbers of more than 78 million Americans and may also have obtained protected health information. *See Anthem Breach*, *supra*. Likewise, in the Equifax data breach, Chinese military hackers working for the People's Liberation Army (PLA) obtained the highly sensitive personal data of 145 million Americans—nearly half the

U.S. population—potentially including financially sensitive creditworthiness information. *See, e.g., Equifax Breach*, *supra*; *see also* Criminal Indictment, *United States v. Zhiyong*, 1:20-cr-00046, Doc. 1 (N.D. Ga. Jan. 28, 2020). And in the Marriott hack, Chinese hackers working for the Ministry of State Security, a key CCP intelligence agency, obtained the personal details of approximately 500 million guests at the "top hotel provider for American government and military personnel," including hotel stays and passport information. *See* Sanger, *supra*.

Collectively, the Chinese government has access to information about Americans' day-to-day routines from TikTok—cataloguing who these Americans interact with, what they do, and where they go—as well as access to many of these individuals' most sensitive personal information. *See US House passes bill that would ban TikTok*, Live Now Fox (Mar. 13, 2024) (statement of Jamil Jaffer), https://perma.cc/9M77-TQNW. The CCP can exploit this massive trove of sensitive data to power sophisticated artificial intelligence (AI) capabilities that can then be used to identify Americans for intelligence collection, to conduct advanced electronic and human intelligence operations, and may even be weaponized to undermine the political and economic stability of the United States

and our allies. *Id.; see also* Sanger, *supra* ("Such information is exactly what the Chinese use to … build a rich repository of Americans' personal data for future targeting."). Indeed, according to former CIA Director Gen. (Ret.) Michael Hayden, speaking about the OPM data breach specifically, there isn't "recovery from what was lost…[i]t remains a treasure trove of information that is available to the Chinese until the people represented by the information age off[]…[t]here's no fixing it." Dan Verton, *Impact of OPM breach could last more than 40 years*, FEDSCOOP (July 10, 2015), https://perma.cc/E6QH-JHLU. The combined national security impact of these hacks—when added to the sensitive social networking, location, and behavioral information on 170 million Americans available to the Chinese government through its direct access to TikTok data—is thus nearly impossible to overstate.

And it only gets worse. The CCP also uses TikTok as both a propaganda and misinformation tool to wield influence over Americans by pushing specific CCP-chosen content while hiding its source. Indeed, most young Americans today do not use TikTok simply to watch or "promote weird dance videos." *The Select: 'TikTok Special,' supra* (statement of Chairman Gallagher). To the contrary, TikTok is the "dominant news

platform for Americans under 30." *Id.*; *see also* TikTok.Br. 41. Given the CCP's external and internal influence over ByteDance and TikTok, the reliance by young people on TikTok for their daily news feed ensures that the CCP maintains editorial control over the content it gets tens of millions of American young people to consume every single day.

TikTok and ByteDance also have the power to boost certain videos and themes through their proprietary and confidential recommendation algorithm providing CCP officials yet another methodology for shaping the content seen and shared by American TikTok users. *See* Emily Baker-White, *TikTok's Secret 'Heating' Button Can Make Anyone Go Viral*, Forbes (Jan. 20, 2023), https://perma.cc/RW78-KTV9. For example, TikTok sent 170 million Americans a prompt encouraging them to call their representatives in Congress to oppose the very legislation before this Court. Maheshwari & McCabe, *supra*. This lobbying effort—created and driven by ByteDance, a CCP-proxy—prompted a "flood of phone calls" to congressional offices to oppose a purported "TikTok shutdown." *Id.* This example alone underscores how the CCP can deploy TikTok as a highly effective propaganda and misinformation tool to influence American policy debates.

Likewise, there is strong evidence that the TikTok content algorithm is built to effectuate the interests of the CCP and to limit content that might undermine its interests. For example, in 2023, the Network Contagion Research Institute released a report highlighting that the TikTok recommendation algorithm regularly down-prioritized content critical of the Chinese regime or supportive of the Hong Kong protestors. *A Tik-Tok-ing Timebomb*, NCRI and Rutgers Miller Center (Dec. 2023), https://perma.cc/4RFG-69RE; *see also* Fergus Ryan, et al., *TikTok and WeChat: Curating and Controlling Global Information Flows*, Australian Strategic Policy Institute (2020), https://perma.cc/K3SF-DH2H. Such decisions are not random and instead point to a concerted effort by TikTok and ByteDance to effectuate the CCP's goals and interests.

Similarly, the TikTok algorithm at times seeks to undermine American and allied interests. For example, in November 2023, in the aftermath of the horrific October 7 terrorist attacks conducted by Hamas in Israel, a flood of videos, one feeding off the other, praising Osama bin Laden's 2002 "Letter to America," were promoted across American feeds by the TikTok algorithm. *See* Donie O'Sullivan, et al., *Some young Americans on TikTok say they sympathize with Osama bin Laden*, CNN (Nov.

16, 2023), https://perma.cc/D6ST-9UL7. Without access to TikTok's proprietary algorithm, lawmakers questioned whether TikTok—controlled by the CCP—was affirmatively boosting the video. Alexander Ward & Matt Berg, *Why bin Laden's letter went viral on social media*, Politico (Nov. 16, 2023), https://perma.cc/4FSS-QYEW. Regardless whether TikTok affirmatively boosted the videos, two prominent Australian researchers recently explained that the Bin Laden incident demonstrates how "TikTok adds a force multiplier effect for disinformation [campaigns]" and noted that "[w]ith more than two billion TikTok users, a strategically crafted misinformation campaign can have a high chance of success," highlighting the "potential for [such videos]…to be[] a severe national security threat and have dangerous consequences." Sascha-Dominik (Dov) Bachmann & Dr. Mohiuddin Ahmed, *Bin Laden's "Letter to America": TikTok and Information Warfare*, Aus. Inst. of Int'l Affairs (Dec. 1, 2023), https://perma.cc/4Y5D-NGCH.

Each of these aspects of Chinese control over TikTok—the massive information gathering efforts, the internal pressure and control over company policy, the use of TikTok in combination with the fruits of CCP-coordinated hacking efforts, and the propaganda machine—is

independently problematic from a national security perspective. Together, they demonstrate that Chinese control of TikTok "poses a clear and present threat to America." *The Select: 'TikTok Special,' supra*.

II. The Act is a measured step to resolve the national security concerns posed by the Chinese government's control of TikTok.

The record here is "replete with evidence" of the national security harms posed by the Chinese government's ownership of TikTok. *See Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 252 (1964); *Hamdi v. Rumsfeld*, 542 U.S. 507, 539 (2004). The Executive Branch and bipartisan majorities in Congress have highlighted these concerns and worked to address them directly. Because TikTok has failed to meaningfully address these concerns, Congress passed the Act, and the President signed it into law specifically to address the grave national security harms threatened by Chinese control over TikTok.

A. The political branches have flagged the national security concerns posed by Chinese control of TikTok.

The Executive Branch. The Executive Branch has been raising concerns about TikTok for years. In 2019, CFIUS reviewed ByteDance's acquisition of musical.ly, citing national security concerns. *President's Decision Regarding the Acquisition by ByteDance Ltd. of the U.S.*

Business of muical.ly, U.S. Dep't of Treasury (Aug. 14, 2020). Following this review, and pursuant to statutory authority, President Trump ordered ByteDance to divest certain assets "used to enable or support ByteDance's operation of the TikTok application in the United States." *Statement by Secretary Steven T. Mnuchin Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297, 51297 (Aug. 14, 2020); *see also Addressing the Threat Posed by TikTok*, 85 Fed. Reg. 48637-38 (Aug. 6, 2020). In the Executive Order, the President described how TikTok's data collection "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information." *Id.* at 48637. Specifically, the President explained that this data would allow "China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." *Id.*

While President Biden revoked this Order in favor of taking other action, he continued to press the issues arising at the intersection of national security and data collection, including specifically addressing the threat posed by TikTok and ByteDance. *See Protecting Americans' Sensitive Data from Foreign Adversaries*, 86 Fed. Reg. 31423 (June 9, 2021).

Following the passage of legislation on the use of TikTok on government devices, White House rapidly implemented guidance to effectuate the removal of TikTok from government devices. *See* Memorandum for the Heads of Executive Departments and Agencies, *"No TikTok on Government Devices" Implementation Guidance*, OMB, M-23-13 (Feb. 27, 2023) (OMB TikTok Guidance); *see also* Pub. L. No. 117-328, div. R, §§ 101-02. The Administration also explained that it had "serious concerns" with TikTok and would continue to look "at other actions" it could take. *Press Gaggle by Principal Deputy Press Secretary Olivia Dalton*, White House Briefing Room (Feb. 28, 2023), https://perma.cc/92PD-SQ66. And shortly after TikTok was banned from government devices, President Biden stated that he would sign a bill banning TikTok altogether. *Remarks by President Biden Before Air Force One Departure*, White House Briefing Room (Mar. 8, 2024), https://perma.cc/58NG-4YAP.

Moreover, in his latest Executive Order regarding data collection issued less than six months ago, President Biden announced new proposals to regulate the type of data that "countries of concern," like China, have access to through applications like TikTok. *See Preventing Access to American's Bulk Sensitive Personal Data*, 89 Fed. Reg. 15780 (Feb. 28,

2024). The President specifically described how access to such data allows these countries of concern to engage in "malicious activities" like "espionage, influence, kinetic, or cyber operations." *Id.* at 15781. And under President Biden, the Department of Justice has continued to defend its authority over ByteDance and TikTok in the musical.ly acquisition before this Court. *See* Petition for Review, *TikTok Inc. v. CFIUS*, No. 20-1444, Doc. 1870778 (D.C. Cir. 2020).

Members of the Executive Branch have also repeatedly testified before Congress and warned the American public in detail about the grave national security threats posed by Chinese control of TikTok as well as ByteDance's direct links to the CCP. *See, e.g.*, *2023 Threat Assessment Hearing*, *supra*; *Homeland Security Secretary on TikTok's Security Threat*, Bloomberg (May 29, 2024) (interview with Secretary Mayorkas), https://perma.cc/W7PQ-68XH; *Fireside Chat with DNI Haines*, DNI Office (Dec. 3, 2022), https://perma.cc/L6AY-TL4D.[1] Between the Executive

[1] *See, e.g.*, *FBI Chief Says TikTok 'Screams' of US National Security Concerns*, Reuters (Mar. 9, 2023), https://perma.cc/F5WC-7AF3; Cecelia Smith-Schoenwalder, *5 Threats FBI Director Wray Warns the U.S. Should Be Worried About*, U.S. News (Jan. 31, 2024) (statement of Director Wray), https://perma.cc/D3B6-Y3UR.

Orders, testimony, and its public statements, as well as its filings in litigation brought by TikTok itself, the Executive Branch has repeatedly made clear its national security concerns regarding TikTok.[2]

Congress. Congress has likewise been quite direct and clear about its national security concerns. Elected officials from both sides of the aisle have expressed deep concerns with TikTok's data collection practices.[3] For example, Senator Warner (D-VA) and Senator Thune (R-SD) explained that TikTok can "enable surveillance by the Chinese Communist Party, or facilitate the spread of malign influence campaigns in the U.S." Press Release, *Senators Introduce Bipartisan Bill to tackle National Security Threats from Foreign Tech* (Mar. 7, 2023), https://perma.cc/X95L-4CD6. In the House of Representatives, Representative Gallagher (R-WI) and Representative Krishnamoorthi (D-IL) stated that "[s]o long as

[2] Independent agency leaders have express similar concerns. *See* Bethany Allen-Ebrahimian, *FCC commissioner says government should ban TikTok*, Axios (Nov. 1, 2022), https://perma.cc/WA2Y-XA76.

[3] *See, e.g.*, *Letter from TikTok Inc. to Senators Blumenthal and Blackburn* (June 16, 2023), perma.cc/4WXM-VR24; *Written Testimony of Geoffrey Cain on Social Media's Impact on Homeland Security*, U.S House of Representatives, Homeland Security and Governmental Affairs Committee (Sept. 14, 2022), https://perma.cc/UDW5-PWW4; *Deputy attorney general warns against using TikTok, citing data privacy*, ABCNews (Feb. 16, 2023), perma.cc/GKK7-BX9D.

[TikTok] is owned by ByteDance…TikTok poses critical threats to our national security." Press Release, *Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans from Foreign Adversary Controlled Applications, Including TikTok* (Mar. 5, 2024) ("*Gallagher Press Release*"), https://perma.cc/6NHJ-ZQCJ. Likewise, the Congressional Research Service has written several reports on the critical privacy and security issues in play with respect to TikTok.[4] And Congress held several hearings and briefings on the matter.[5] At these hearings, members of Congress, like Senator Rubio, expressed specific concerns about how the

[4] *See, e.g.*, *TikTok: Recent Data Privacy & Nat'l Security Concerns*, IN12131 (Mar. 29, 2023), https://perma.cc/9E94-3C25; *TikTok: Technology Overview & Issues*, R46543 (Updated June 30, 2023), https://perma.cc/U9SD-98EM; *Restricting TikTok (Part I): Legal History & Background*, LSB10940 (Updated Sept. 28, 2023), https://perma.cc/UV27-YBRL; *Restricting TikTok (Part II): Legislative Proposals & Considerations for Congress*, LSB10942 (Updated Mar. 15, 2024), https://perma.cc/PMW2-2QUB; *TikTok: Frequently Asked Questions & Issues for Congress*, R48023 (Apr. 9, 2024), https://perma.cc/U2Q8-3L3N.

[5] *See, e.g.*, *2023 Threat Assessment Hearing* at 1:09:00, *supra*; *Testimony of Shou Chew*, H. Comm. on Energy & Commerce, No. 118-13, 118th Cong., 1st Sess. (Mar. 23, 2023), https://perma.cc/6G5S-K77A; *Hearing Memorandum*, H. Comm. on Energy & Commerce, No. 118-13, 118th Cong., 1st Sess. (Mar. 20, 2023), https://perma.cc/3EV6-7AZA; *2023 House Data Privacy Hearing*, *supra*; *Protecting Americans from Foreign Adversary Controlled Applications*, H. Rep. 118-417, 118th Cong., 2d Sess. 1 (Mar. 11, 2024), https://perma.cc/9S3H-GME8.

CCP manipulates information fed through TikTok and argued that the application "is probably one of the most valuable surveillance tools on the planet." *2023 Threat Assessment Hearing* at 1:09:00, *supra*.

Indeed, it was concerns about the CCP and its activities targeting Americans that convinced the House of Representatives to establish the Select Committee on Strategic Competition between the United States and the CCP. The China Select Committee, as it is colloquially known, has repeatedly sounded the alarm over the national security threat posed by TikTok. *See, e.g., Rep. Gallagher Letter*, *supra*. Specifically, the China Select Committee has noted that "the Chinese Communist Party—and its leader Xi Jinping, have their hands deep in the inner workings of" TikTok," explaining that ByteDance "is legally required to support the work of the Chinese Communist Party." *See Press Conference to Introduce the Protecting Americans from Foreign Adversary Controlled Applications Act*, China Select Committee (Mar. 6, 2024) (statement of Chairman Gallagher), https://perma.cc/NBC3-H3PB.[6] Likewise, during a China

[6] The States, too, have long been investigating TikTok under their consumer and child protection laws, police powers, and their authority to protect state systems and critical infrastructure. *See, e.g.*, David Shepardson, *State AGs demand TikTok comply with US consumer protection*

Select Committee hearing to discuss the CCP's support for America's adversaries, former Secretary Pompeo described TikTok as engaging in "information warfare" because it delivers different content to Americans than it does to individuals in China. *See Transcript of Hearing on Authoritarian Alignment*, China Select Committee (Jan. 30, 2024), https://perma.cc/XQD2-578Z.

B. TikTok has failed to respond to these legitimate concerns.

Despite these public concerns, TikTok itself has repeatedly failed to effectively address legitimate questions from Congress and others on how it collects, stores, and shares data, including sensitive personal data of Americans. *See 2023 House Data Privacy Hearing*, *supra*. And the fact

---

investigations, Reuters (Mar. 6, 2023), perma.cc/9NL6-2VPW; Justine McDaniel, *Indiana sues TikTok, claiming it exposes children to harmful content*, Washington Post (Dec. 7, 2022), perma.cc/V2RV-AU3P; *see also, e.g.*, *ICYMI: Attorney General Austin Knudsen Joined Krach Institute to Discuss Montana's TikTok Ban and Chinese Spy Balloon*, Montana Dep't of Justice (Sept. 28, 2023), https://perma.cc/UN8H-2ZNL; *Attorney General Miyares Leads 18 State Coalition Supporting Montana's TikTok Ban*, Office of the Virginia Attorney General (Sept. 19, 2023), https://perma.cc/27R8-2DAY. Indeed, as of March 2024, thirty-nine States have barred TikTok from government devices, citing concerns about the security of state and critical infrastructure systems as well as state government data. *See* Cailey Gleeson, *These 39 States Already Ban TikTok From Government Devices*, Forbes (Mar. 12, 2024), https://perma.cc/T7Y4-XJY9.

that China "has made clear in public statements that it would not permit a forced divestment," only reinforces these concerns. TikTok.Br. 2.

For example, at a congressional hearing last year, TikTok's CEO acknowledged that some China-based employees continue to have access to U.S. data, including sensitive personal data of Americans. Lauren Feiner, *TikTok CEO says China-based ByteDance employees still have access to some U.S. data*, CNBC (Mar. 23, 2023), https://perma.cc/9LU9-JBAN. Moreover, when pressed, TikTok's CEO could not say whether TikTok sells data to other entities or whether the Chinese government exerts influence over TikTok. *See* Louis Casiano & Hillary Vaugh, *TikTok CEO refuses to answer if Chinese government has influence over platform as Congress mulls ban*, Fox Business (Mar. 14, 2024), https://perma.cc/8BCT-ERTL; Ken Tran & Rachel Looker, *What does TikTok do with your data?*, USA Today (Mar. 23, 2023), https://perma.cc/2LVQ-3Z6L. And when asked whether ByteDance has an internal CCP committee, the TikTok CEO punted, responding, "[l]ike I said, all businesses that operate in China have to follow the law." *See* D. Wallace, *TikTok CEO grilled on Chinese Communist Party influence*, Fox Business (Jan. 31, 2024), https://perma.cc/KJ9F-8HJ7. The inability

of senior TikTok leaders to effectively allay the basic concerns of American lawmakers only reinforces the pervasive and unique threat that TikTok poses to Americans and our national security.

C. Project Texas does not mitigate the risks or address the ongoing harms.

Finally, TikTok's efforts to appease U.S. lawmakers through a plan to retain American data wholly in the United States (aka "Project Texas") have likewise failed to meaningfully eliminate key national security concerns. While the physical location of data storage for American user may conceivably alleviate *some* concerns, what really matters is the "leverage" China "has over the people who have access to that data." *See* D. Harwell & T. Room, *Inside TikTok*, Washington Post (Nov. 5, 2019), https://perma.cc/B368-JNN4 . Contrary to TikTok's claims about how Project Texas would protect American data and limit the threat posed to Americans from potential disinformation efforts, TikTok's own repeated statements reveal that the CCP continues to have access to user data stored in America and exercises deep influence on—and control over—TikTok's internal decision making. Indeed, TikTok "[m]anagers told employees that they actually could save data to their computers, and that there would be exceptions" to Project Texas's data sharing restrictions.

Georgia Wells, *TikTok Struggles to Protect U.S. Data from Its China Parent*, WSJ (Jan. 30, 2024), https://archive.is/a8LtA.

As long as TikTok continues to use its own algorithm—developed and managed in China—the CCP is bound to be able to access data, regardless where it is stored. As one TikTok employee stated, "[i]t remains to be seen if at some point product and engineering can still figure out how to get access, because in the end of the day, it's their tools." *See* Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, Buzzfeed (June 17, 2022), https://perma.cc/7LF4-Y3XD. Indeed, while Project Texas may look good on paper, former employees have said the project has been mostly "cosmetic" and has failed to address the core concerns over the application and CCP access to American data. *See* Gaby Del Valle, *Report: TikTok's effort to silo US data 'largely cosmetic'*, The Verge (Apr. 16, 2024), https://perma.cc/WR45-NZCU.

In sum, after months of digging deep into TikTok and its operations, it was clear to key Congressional leaders that TikTok fundamentally functions as an arm of the CCP in both promoting and censoring data in the interests of the CCP. And because TikTok fails to meaningfully

address the national security concerns, Congress was forced to step in and take action.

D. Congress passed the Act to resolve the national security concerns posed by Chinese control of TikTok.

The Act addresses these precise concerns. In March 2024, the bi-partisan leadership of the China Select Committee, along with other key members of the House, introduced legislation that became the genesis for the legislation challenged in this matter. *See* Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024); *see also Gallagher Press Release*, *supra*. Relying on the extensive record built over the preceding months as it conducted its deep dive into the national security threat posed by TikTok, the legislation—which was incorporated into a foreign aid package—easily passed the House and Senate. Roll Call 145: H.R. 8038, Clerk of the United States House of Representatives, 118th Cong.(Apr. 20, 2024) (passing the House with a vote of 360-58); Roll Call 154: H.R. 815, United States Senate, 118th Cong. (Apr. 23, 2024) (passing the Senate with a vote of 79-18). President Biden signed the bill into law the following morning. *See* H.R. 815, 118th Cong., Congress.gov (Apr. 24, 2024). This legislation—which only requires divestment by ByteDance of the TikTok application—and does not effectuate any restrictions on TikTok's availability if

divestiture happens—is a measured and sensible response to the national security threat posed by TikTok. *See* Pub. L. No. 118-50.

III. The government's compelling national security interests overcome any applicable level of First Amendment scrutiny.

Having failed to effectively confront the enduring national security threat that TikTok and its relationship with the CCP poses to American's and their data, TikTok now seeks to wrap itself in the American flag, citing the First Amendment as the core reason the government ought not be able to force divestiture. *See* TikTok.Br. 28-38. However, as the United States correctly explains, the Act does not even implicate the First Amendment. *See* USA.Br. 59. This is because the Act doesn't target *any protected speech* nor a*nyone with free speech rights*. Rather, it targets the CCP's control of TikTok, and requires divestiture by its Chinese owners if TikTok is to continue to enjoy unabated access to the sensitive personal data of over 170 million Americans. See USA.Br. 1-3. Contrary to TikTok and ByteDance's claims that there is something unique or untoward going on here, the federal government has long regulated foreign ownership and control of companies operating in all sorts of industries. *See, e.g.*, 12 U.S.C. §72 (nationally chartered banks); 16 U.S.C. §797 (dams, reservoirs, and similar projects); 42 U.S.C. §§2131-34 (nuclear facilities); 49

U.S.C. §§ 40102(a)(15), 41102(a) (air carriers). Indeed, the federal government has long regulated foreign ownership telecommunications assets and media, including radio and broadcast television licenses, for nearly identical reasons. 47 U.S.C. § 310(b)(3) (radio and broadcast television); *see Pacific Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023). In *Pacific Networks*, just last year, this Court upheld the FCC's revocation of authorizations for Chinese telecommunications companies to operate communications lines in the United States because Chinese control of such companies "provid[ed] opportunities for … the Chinese government to access, monitor, store, and in some cases disrupt [or] misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States." *Id.* at 1162-63; *see also China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 265-66 (D.C. Cir. 2022).

Moreover, even if there is some expressive content on the TikTok platform that would be adversely affected by a required divesture—although TikTok fails to explain what such content might be—Congress can regulate TikTok's pervasive and widespread collection of Americans' personal data, which is not itself expressive activity. *See Sorrell v. IMS*

Health, Inc., 564 U.S. 552, 567 (2011) ("[T]he First Amendment does not prevent restrictions direct at commerce or conduct from imposing incidental burdens on speech."); *Haig v. Agee*, 454 U.S. 280, 307 (1981) ("[N]o governmental interest is more compelling than the security of the Nation."). And even if TikTok's recommendation algorithm might be viewed as having some expressive function, in that it ostensibly engages in an editorial function by curating content, such speech is unprotected because it is the speech of foreign entities—ByteDance, TikTok Global, and the CCP—none of whom are entitled to First Amendment protection. *See Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 591 U.S. 430, 436 (2020) ("[P]laintiffs' foreign affiliates possess no rights under the First Amendment."); *see* USA.Br. 59-60. And while TikTok US may be incorporated in the United States, TikTok has made clear that the technology fueling its algorithm is developed in China and is ultimately controlled by its Chinese parent company, ByteDance, which, in turn, faces inexorable pressure—and control—by the CCP. *See* TikTok.Br. 24. Nothing in the First Amendment can be read to shield the covert influence or intelligence collection efforts of a foreign government targeting the American people.

The only even *arguably* protected speech that might even *theoretically* be affected is that of American content creators and (perhaps) any content moderation performed by TikTok US that is done completely separate and apart from TikTok's CCP-dominated recommendation algorithm. There are, of course, a number of reasons why this theoretical impact is not actionable. First, speech rights are personal and cannot be raised vicariously by others as TikTok seeks to do in this litigation. *Broadrick v. Oklahoma*, 413 U.S. 601, 610-11 (1973); *see also Murthy v. Missouri*, 144 S. Ct. 1972, 1996 (2024). Second, TikTok has repeatedly made clear that its content moderation is driven primarily by the core TikTok algorithm, which is not only built in and controlled by Chinese entities but is actually significantly responsive to the goals and interests of the CCP. *See, e.g.*, *A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives*, NCRI and Rutgers Miller Center (Dec. 2023), https://perma.cc/4RFG-69RE; *see also* Fergus Ryan, *supra*. Third, to the extent content creators present in this litigation might validly raise their own First Amendment claims, the fact is that while the First Amendment may protect relevant expressive activity and content, it does not

guarantee a particular venue for such speech—particularly when the venue is a private forum, not a public space controlled by the government—and even where it is, the government can impose in reasonable content-neutral time, place, and manner restrictions so long as they are content-neutral. *See Heffron v. International Soc'y for Krishna Consciousness, Inc.*, 452 U.S. 640, 647 (1981); *Kovacs v. Cooper*, 336 U.S. 77, 88-89 (1949). And finally, the availability of a wide and diverse range of alternative venues for American speech—from Instagram to YouTube and beyond—must weigh into any analysis of the claimed infringement of speech rights. *See, e.g.*, *Ward v. Rock Against Racism*, 491 U.S. 781, 802 (1989).

And even if these issues were not themselves insurmountable barriers to TikTok's failed effort to hide behind the U.S. Constitution, the fact that the Act doesn't actually inhibit *any* speech is just such a barrier. Rather than barring speech, as the government correctly points out, "Congress expressly authorized the continuation of [] expressive activities on TikTok so long as the national-security harms could be mitigated." *See* USA.Br. 60.

The Act thus has only an incidental—if any—impact on arguably protected speech. Under longstanding precedent, the Act is therefore lawful so long as it is "within the constitutional power of the Government [and] furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *United States v. O'Brien*, 391 U.S. 367, 377 (1968).

The Act easily meets this test. To begin with, the Framers understood national security to be the "principal purpose[]" of government. The Federalist No. 23 (Alexander Hamilton); *see also* Federalist Nos. 34, 41. The Constitution therefore confers upon Congress robust national-security authority, *see, e.g.*, U.S. Const. art. I, §8, cl. 3, 11, 12, 13 (to regulate foreign commerce, declare war, raise and support armies and the Navy), and vests the President with "[t]he executive Power," establishes him as the "Commander in Chief," *id.* art. II, §1 & §2, cl.1, and making him the Nation's "'sole organ'" in foreign affairs. *Zivotofsky ex rel. Zivotofsky v. Kerry*, 576 U.S. 1, 20 (2015) (quoting *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936)).

And as the examples above illustrate, *see supra* at 20-21, it is well established that regulating foreign ownership and control of companies operating within the United States—particularly in the media and telecommunications industries—is within the scope of these broad powers. The Act thus falls safely "within the constitutional power of the Government." *O'Brien*, 391 U.S. at 377. Further, the government's national security interest in preventing "the national-security harms that accompany China's ability to exploit TikTok," USA.Br. 59, is "unrelated to the suppression of free expression," *O'Brien*, 391 U.S. at 377, especially because, as noted above, the Act requires divestment of TikTok and nothing more. For the same reason, any incidental burden on protected speech is no "greater than is essential to the furtherance of [the Government's national security] interest," *id.*, especially because "[a]ny TikTok users in the U.S." who might feel some incidental burden on their speech "have the option of turning to other platforms." *See* USA.Br. 60; *see Heffron*, 452 U.S. at 647 ("[T]he First Amendment does not guarantee the right to communicate one's views at all times and places or in any manner that may be desired.").

This is the case regardless of what level of First Amendment scrutiny might be applied. The Act's divestment remedy is narrowly tailored to address the specific national security harms threatened by Chinese control of TikTok as well the government's interest in protecting more than 170 million Americans from the theft and misuse of their sensitive personal data by proxies of a foreign nation-state and the CCP's covert influence efforts. These matters are not simply *a* compelling interest, but perhaps *the most* compelling interest. *See Haig*, 453 U.S. at 307.

CONCLUSION

For these reasons, the petitions should be denied.

Dated: August 2, 2024

Respectfully submitted,

/s/ Thomas R. McCarthy

Thomas R. McCarthy
Kathleen S. Lane
Consovoy McCarthy PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com
katie@consovoymccarthy.com

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 29(a)(5) because it contains 6,497 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)–(6) because it was prepared using Microsoft Word in Century Schoolbook 14-point font, a proportionally spaced typeface.

Dated: August 2, 2024

/s/ Thomas R. McCarthy
Thomas R. McCarthy

Counsel for Amici Curiae

APPENDIX A: LIST OF AMICI CURIAE

The Hon. Michael B. Mukasey
Former Attorney General of the United States
Former Judge, United States District Court for the Southern District of New York

The Hon. Jeff Sessions
Former Attorney General of the United States
Former United States Senator

The Hon. Chris Inglis
Former National Cyber Director, The White House
Former Deputy Director, National Security Agency

The Hon. Christopher A. Ford
Former Assistant Secretary of State for International Security & Non-proliferation, United States Department of State
Former Senior Director for Weapons of Mass Destruction & Counterproliferation, National Security Council, The White House

The Hon. Michelle Van Cleave
Former National Counterintelligence Executive, Office of the Director of National Intelligence
Former General Counsel and Assistant Director, Office of Science and Technology Policy, The White House

The Hon. William Evanina
Former Director, National Counterintelligence and Security Center

Gus P. Coldebella
Former General Counsel (acting), United States Department of Homeland Security

Margaret M. Peterlin
Former Chief of Staff to the Secretary of State, United States Department of State

Former National Security Advisor to the Speaker of the House, United States House of Representatives

Vice Admiral (Ret.) Mike LeFever
Former Director of Strategic Operational Planning, National Counter-terrorism Center, Office of the Director of National Intelligence
Former Commander of the Office of Defense Representative in Pakistan & Commander of the Joint Task Force in Pakistan

Norman T. Roule
Former National Intelligence Manager for Iran, Office of the Director of National Intelligence
Former Division Chief, Central Intelligence Agency

Dr. Lenora P. Gant
Former Assistant Deputy Director of National Intelligence for Human Capital, Office of the Director of National Intelligence
Former Senior Executive for Academic Outreach and Science, Technology, Engineering, and Mathematics & Senior Advisor to the Research Directorate, National Geospatial-Intelligence Agency

Paula Doyle
Former Associate Deputy Director for Operations Technology, Central Intelligence Agency
Former Deputy National Counterintelligence Executive, Office of the Director of National Intelligence

Teresa H. Shea
Former Signals Intelligence Director, National Security Agency

Michael Geffroy
Former General Counsel, Senate Select Committee on Intelligence, United States Senate
Former Deputy Chief of Staff and Chief Counsel, Committee on Homeland Security, United States House of Representatives

Geof Kahn
Former Senior Advisor to the Director of Central Intelligence, Central Intelligence Agency
Former Policy Director & CIA Program Monitor, House Permanent Select Committee on Intelligence, United States House of Representatives

Jamil N. Jaffer
Former Chief Counsel & Senior Advisor, Senate Foreign Relations Committee, United States Senate
Former Associate Counsel to President George W. Bush, The White House

Rick "Ozzie" Nelson
Former Director, Joint Interagency Task Force, Joint Special Operations Command
Former Group Chief, National Counterterrorism Center

Andrew Borene
Former Senior Officer, Office of the Director of National Intelligence
Former Associate Deputy General Counsel, Department of Defense

Edward Fishman
Former Member, Policy Planning Staff, Office of the Secretary of State, United States Department of State
Former Russia and Europe Sanctions Lead, United States Department of State