

Statement for the Record
of
Jamil N. Jaffer¹
on
How the CCP Uses the Law to Silence Critics and Enforce its Rule
before the
United States House Select Committee on the Chinese Communist Party

September 19, 2024

I. Introduction

Chairman Moolenaar, Ranking Member Krishnamoorthi, and Members of the Committee: thank you for inviting me here today to discuss the Chinese Communist Party’s (CCP) use of the law—and specifically its exploitation of the American legal system—to enforce its rule at home, silence its critics abroad, and benefit itself at the expense of the American people and our allies.

I want to thank the Chairman and Ranking Member for holding this particular hearing, given the ongoing pressure currently focused on leading American experts and companies with the threat of litigation or other punitive actions, whether in our courts or elsewhere. These threats are made by the CCP in an effort to force those individuals and organizations to limit their criticism of the CCP or the People’s Republic of China (PRC), which the CCP controls with an iron fist, and their proxy institutions, including but not limited to PRC-state supported enterprises. They are likewise used, oftentimes, to force American and allied companies to engage in business relationships that are ultimately not economically beneficial to them, and which undermine our economic system, including the protection of intellectual property. Your bipartisan leadership on this Committee has been critical to highlighting the many ways that the CCP has sought to take advantage of our nation’s free and open society, as well as that of our allies, to gain political, economic, technological, and military advantage in the context of the larger strategic competition taking place across the globe.

As members of this Committee all too well know, China is the key economic and national security challenge facing our nation going forward, and I hope this hearing will offer us the opportunity to have a candid and frank discussion on these important matters.

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. 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 the House Select Committee on the CCP 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. Mr. Jaffer would like to thank Kelly Crowley, Zach Rosen, and Ann Long for their very helpful research assistance with respect to this testimony.

II. The Threat of a Rising China

As I testified 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.² 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.³ To get an even better sense of the global scale of the CCP's repression, one needs only look at the PRC's near-constant drumbeat of military and economic threats against Taiwan,⁴ its hostile actions and active threats towards other U.S. allies and partners globally,⁵ its export of surveillance technologies and other repressive capabilities to authoritarian-leaning regimes worldwide,⁶ its ongoing efforts to consolidate control over and withhold access to key critical minerals and strategic metals,⁷ its extortion of dozens of countries under the Belt and Road

² See 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>.

³ 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>>.

⁴ 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>>.

⁵ 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/>> (describing the Secretary of the Air Force Frank Kendall's recent speech as explaining “that the 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>>.

⁶ 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>.

⁷ 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

Initiative (BRI),⁸ and its growing political, economic, and military relationships with other global repressors like Russia, Iran, and North Korea.⁹

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,¹⁰ and the PRC's deep and expanding cyber infiltration of U.S. and allied critical infrastructure,¹¹ as well as its active installation of capabilities to hold such critical infrastructure

<<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.* (“Over the last decade, geopolitics have increasingly driven economic policies, leading to increased risks and disruptions in global markets. 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.”).

⁸ *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 Gelpert, 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>>.

⁹ *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/>>.

¹⁰ *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.’”).

¹¹ *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>> (“The U.S. authoring agencies have

at risk,¹² 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 Program¹³ and has sought to shape minds of students through its establishment of hundreds of Confucius Institutes across the globe.¹⁴

Even more perniciously, we know that the CCP, including through its companies and others, is seeking to use the U.S. legal system to also undermine our security. Indeed, Chinese companies regularly seek to hide their hand in litigation in U.S. courts, conceal their assets from litigants, use the bankruptcy system to steal sensitive technology, and threaten academics and other researchers with litigation to chill free speech about the CCP and its shenanigans.

III. The CCP’s Use of Lawfare to Threaten Americans and Other Allies Who Dare to Speak Out Against the PRC.

It is this latter threat—the use of our own system to go after American researchers, scholars, and activists—that is particularly concerning. For example, just three months ago, in June 2024,

confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam....ASD’s ACSC and NCSC-NZ assess Australian and New Zealand critical infrastructure, respectively, could be vulnerable to similar activity from PRC state-sponsored actors.”).

¹² See *id.* (“The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People’s Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States....Volt 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.”)

¹³ 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*, 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”).

¹⁴ 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>>.

Yangtze Memory Technologies Corporation (YMTC)—a company that the United States Department of Defense listed in January 2024 as being a “Chinese Military Compan[y] Operating in the United States” under Section 1260H of the 2021 National Defense Authorization Act¹⁵—sued Dr. Roslyn Layton, a fellow at GMU Scalia Law School’s National Security Institute (NSI, the academic center and think tank that I run) and the founder of a well-known China-focused website, China Tech Threat, for trade libel and other associated claims in D.C. Federal District Court.¹⁶ Dr. Layton, a well-respected expert in the field, has published a number of articles and studies arguing that China poses a national security threat to the United States and its allies,¹⁷ as well as a range of articles on telecommunications regulation, internet governance and the like, including pieces for NSI, on its blog, *The SCIF*.¹⁸ Dr. Layton has likewise appeared on multiple panels and in public appearances, including testimony before Congress, speaking on a range of issues, including the threat that China poses to the American economy and that of our allies, as well as telecommunications, internet, and antitrust policy, including at events hosted by NSI.¹⁹

The YMTC lawsuit, which remains pending, alleges, among other things, that a June 2022 report co-authored by Dr. Layton, “falsely brands YMTC as a ‘Chinese Military Chip Maker’...[and] further propagate[s] the myth that YMTC’s memory products pose security and privacy risks to U.S. consumers.”²⁰ The Complaint—filed in June 2024 for YMTC by DC- and LA-based partners (and an SF-based associate) of Latham & Watkins, a prestigious American law firm—further alleges that “YMTC is not owned or controlled by the Chinese military...has never supplied its technology or products for any military use...[a]nd...has never been directed by any entity to supply its technology or products for military use” and goes on to argue that Dr. Layton “knew (or, at a minimum, recklessly disregarded) the falsity of [her] baseless statements,” suggesting that Dr. Layton sought to “creat[e] an echo chamber of misinformation” and to “complet[e] [her] circle of lies.” While the Federal District Court in the District of Columbia will ultimately weigh in on the merits of YMTC’s lawsuit, it is worth noting that, at least based on its

¹⁵ See United States Department of Defense, *Entities Identified as Chinese Military Companies Operating in the United States in accordance with Section 1260H of the William M. (“Mac”) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)* (Jan. 31, 2024), at 3, available online at <<https://media.defense.gov/2024/Jan/31/2003384819/-1/-1/0/1260H-LIST.PDF>> (listing “Yangtze Memory Technologies Co., Ltd. (YMTC)” as a newly listed CMC operating in the United States on page 3).

¹⁶ See Complaint, *Yangtze Memory Technologies Company, Ltd. and Yangtze Memory Technologies, Inc. v. Strand Consult and Roslyn Layton*, Case No. 5:24-cv-3454-BLF, Document 1 (filed June 7, 2024).

¹⁷ See, e.g., Dr. Roslyn Layton & Jeff Ferry, *Silicon Sellout: How Apple’s Partnership with Chinese Military Chipmaker YMTC Threatens National Security*, China Tech Threat & Coalition for a Prosperous America (June 2022), available online at <<https://chinatechthreat.com/wp-content/uploads/2022/06/Silicon-Sellout.-How-Apples-Partnership-With-Chinese-Military-Chip-Maker-YMTC-Threatens-National-Security.pdf>>.

¹⁸ See, e.g., Dr. Roslyn Layton, *Imposing Section 214 Creates Busy Work, Not Improved National Security* (Blog Post), The SCIF (Mar. 26, 2024), available online at <<https://thescif.org/imposing-section-214-creates-busy-work-not-improved-national-security-d6175b2b57e3>>; Dr. Roslyn Layton, *As China Looks to 6G, the U.S. has No Spectrum Auctions, No Pipeline, and No Plan* (Blog Post), The SCIF (July 21, 2023), available online at <<https://thescif.org/as-china-looks-to-6g-the-u-s-has-no-spectrum-auctions-no-pipeline-and-no-plan-31c033fbf2a>>.

¹⁹ See, e.g., Dr. Roslyn Layton, et al., *The National Security Implications of Antitrust: America’s Allies*, National Security Institute (Sept. 23, 2021), available online at <<https://nationalsecurity.gmu.edu/the-national-security-implications-of-antitrust-americas-allies/>>.

²⁰ See Complaint, *YMTC v. Layton*, *supra* n. 16 at p. 3, ¶ 6.

statutory determination made in January 2024, the Department of Defense would appear to disagree with YMTC’s position, a fact not mentioned by YMTC or its prestigious American lawyers even once in their complaint, notwithstanding that the complaint was filed nearly six months after the public release of DOD’s determination.

Likewise, today you will hear from my fellow panelist, Anna Puglisi, a scholar at the Hoover Institution at Stanford University (and a former U.S. National Counterintelligence Officer for East Asia)²¹ about her experience receiving cease-and-desist letters from multiple Chinese companies, including BGI, based on a paper she wrote in May 2024 while a Senior Fellow at Georgetown University’s Center for Security and Emerging Technology (CSET). Ms. Puglisi, who “advis[ed] senior US and foreign government officials at the highest levels...on counterintelligence issues” at the U.S. National Counterintelligence and Security Center and “played a prominent role in drafting national science and technology strategies and in designing mitigation strategies to protect technology for both the public and private sectors,” while also receiving multiple awards, including the FBI Director’s Award for Excellence, is “a coauthor of the 2013 study *Chinese Industrial Espionage*, the first book-length treatment of the topic, as well as countless related proprietary studies...[and] is proficient in Mandarin Chinese.”²²

As you’ll hear Ms. Puglisi describe in her own words, for her work on how the PRC’s support of companies like BGI skews competition in the biotech market, like Dr. Layton, Ms. Puglisi received a cease-and-desist letter in June 2024 from a DC-based partner of Steptoe & Johnson, another prominent American law firm representing BGI. The letter threatened legal action against Ms. Puglisi and Georgetown University should she fail to retract her statements about the company, which BGI alleged were false and defamatory. This letter, as you will hear from Ms. Puglisi, also resulted in Georgetown University refusing—at least to this point—to indemnify Ms. Puglisi’s defense, notwithstanding the fact that her paper was subject to multiple peer reviews and fact-checking before publication.

And recently, as these efforts were being launched by Chinese companies and their American lawyers against Dr. Layton and Ms. Puglisi, TikTok, a major social media platform that serves over 170 million Americans, went after State Armor Action, “a 501(c)(4) non-profit organization working to expose malign Chinese Communist Party influence operations in America’s heartland,” that “advocates in statehouses around the country for state level solutions to the global threats posed by the CCP.”²³ In yet another cease-and-desist effort, lawyers for TikTok apparently threatened legal action against State Armor Action for running a multi-million dollar ad campaign exposing TikTok’s potential for being a powerful propaganda and espionage tool for the CCP.²⁴

²¹ See Anna Puglisi, Visiting Fellow, Hoover Institution, *available online at* <<https://www.hoover.org/profiles/anna-puglisi>>.

²² *Id.*

²³ See State Armor Action, *State Armor Action Launches Multimillion Dollar Campaign Exposing TikTok’s Ties to Chinese Government* (May 24, 2024), *available online at* <<https://www.prnewswire.com/news-releases/state-armor-action-launches-multimillion-dollar-campaign-exposing-tiktoks-ties-to-chinese-government-302094728.html>>.

²⁴ See *id.* (describing State Armor Action’s multimillion dollar campaign).

The very real national security threat posed by TikTok 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.²⁵ That brief, which supported the U.S. government’s position defending the legislation drafted and recommended by this Committee, passed by Congress, and 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.”²⁶

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 30,²⁷ 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 campaigns targeting American citizens and our allies.²⁸ It was because of State Armor Action’s effort to highlight just these type of threats for the American public, that it apparently got its cease-and-desist letter, just like Dr. Layton and Ms. Puglisi.

Were these the only examples of Chinese corporate lawfare against American and allied researchers, one might think they were isolated cases, all taking place in the last year. Unfortunately, the CCP’s use of its proxy companies to go after its most effective critics by threatening legal action in the United States or elsewhere is simply a quickening drumbeat. Indeed, as far back as 2016, the Project 2049 Institute, a 501(c)(3) “nonprofit research organization focused on promoting American values and security interests in the Indo-Pacific region,”²⁹ was threatened by a European law firm retained by the China Energy Fund Committee Europe (CEFC Europe), which alleged that Project 2049’s claim that CEFC’s parent company had ties to the Chinese military through one of its senior leaders was untrue. When Project 2049’s leadership responded with data backing up its claim, however, CEFC apparently went radio silent.

²⁵ 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, 2023) (attached hereto as Exhibit A).

²⁶ *Id.* at 1-7, 11-14.

²⁷ *Id.* at 10-11.

²⁸ *Id.* at 3-10.

²⁹ See Project 2049 Institute, *About Us*, available online at <<https://project2049.net/about/>>.

And in 2020, BYD, the Chinese electric vehicle manufacturer that has—with the help of massive Chinese government subsidies³⁰ and likely preferred access to strategic metals essentially locked up by the Chinese government action—been building some of the world’s largest battery factories in China,³¹ sued the Alliance for American Manufacturing (AAM), a “non-profit, non-partisan partnership formed in 2007 by some of America’s leading manufacturers and the United Steelworkers.”³² The lawsuit, like the claims made against Project 2049 a couple of years earlier, and the actions and threats made against Dr. Layton, Ms. Puglisi, and State Armor Action more recently, alleged that AAM had defamed BYD in a series of public statements.³³ Both the federal district court in D.C. and the D.C. Circuit held that BYD’s claim could not survive a motion to dismiss,³⁴ but it took nearly two years and likely tens of thousands of dollars in litigation expenses, if not more, to win this fight.

And this, perhaps, is the crux of the matter: what these lawsuits and unveiled threats reveal is an extensive effort by the Chinese government and its proxy companies to use our own courts and our legal system to silence American and allied critics who seek to call out the true nature of the Chinese Communist Party and the very real threat it poses to our economic and national security.

IV. The CCP’s Larger Use of Economic Tools and Law to Constrain Behavior at Home and Abroad

Indeed, the CCP government can’t help itself, as it even goes after American politicians who dare critique it or act in ways that it doesn’t like. Not satisfied to go after academics, think tanks, and nonprofits, the Chinese government often sanctions American politicians and policymakers, recently going after the founding Chairman of the China Select Committee, former Congressman Mike Gallagher (R-WI), the Chairman of the House Foreign Affairs Committee, Congressman Michael McCaul (R-TX), and the Ranking Member of the House Rules Committee, Congressman Jim McGovern (D-MA).³⁵

³⁰ See, e.g., Stefan Nicola, *BYD Got €3.4 billion Chinese Aid to Dominate EVs, Study Says*, Bloomberg (Apr. 10, 2024), available online at <<https://www.bloomberg.com/news/articles/2024-04-10/byd-got-3-4-billion-chinese-aid-to-dominate-evs-study-says?embedded-checkout=true>>

³¹ See, e.g., Reuters Staff, *China’s BYD Launches World’s Biggest Battery Factory*, Reuters (June 28, 2018), available online at <<https://www.reuters.com/article/us-china-autos-byd/chinas-byd-launches-worlds-biggest-battery-factory-idUSKBN1JO0SI/>>; see also Jet Sanchez, *BYD Breaks Ground on World’s Largest Sodium-Ion Battery Plant*, Driven Car Guide (Jan. 8, 2024), available online at <<https://www.drivencarguide.co.nz/news/byd-breaks-ground-on-worlds-largest-sodium-ion-battery-plant/>>

³² See Alliance for American Manufacturing, About Us, available online at <<https://www.americanmanufacturing.org/about-us/>>.

³³ See Complaint, *BYD Company Ltd. v. Alliance for American Manufacturing*, Case No. 1:20-cv-03459 (TNM), Document 1 (Filed Nov. 25, 2020).

³⁴ See Order Granting Motion to Dismiss, *BYD v. AAM*, *supra* n. 32, Document 28 (filed Aug. 6, 2021); See Mandate of USA, *BYD v. AAM*, *supra* n. 32, Document 32 (filed June 17, 2022)

³⁵ See, e.g., Huizhong Wu & Didi Tang, *China Sanctions US Rep. McGovern for ‘Interference’ in Its Domestic Affairs*, AP (Aug. 1, 2024), available online at <<https://apnews.com/article/china-sanctions-congress-mcgovern-649c029092175ad14b3d7996d199b7f3>>.

In many ways, this is simply another part of a larger PRC effort to leverage our own institutions against us. One need only look at the behavior of the National Basketball Association (NBA), an iconic American brand which deeply tarnished itself a few years ago after threatening its own coaches and players with discipline for speaking out publicly on a clear matter of conscience: the Chinese government's horrific treatment and incarceration of Muslim Uyghurs.³⁶

Of course, organizations like NSI will not be cowed and will continue to host events like:

- On the Road to Global Repression: China's Tools of Economic Repression
- Countering Chinese Global Tech Ambitions: U.S.-EU Partnership in Smart Innovation
- Surveillance State: China's Digital Tools of Repression
- Tomorrow's Battlefield: How the U.S. Can Win the Tech Competition with China
- 2022 Winter Olympics: Standing Up to China's Human Rights Abuses
- China's Rise: Confronting China's Challenge to the World Order

We will also continue to feature courageous and expert voices on these issues like Enes Kanter Freedom, Joey Siu, Yaqiu Wang, Lindsay Gorman, Geoffrey Cain, Josh Rogin, Rep. Mike Gallagher, Rep. Jennifer Wexton, and Rep. Mike Waltz, to name just a few.

And NSI will continue to publish papers like:

- Addressing the National Security Threat of Chinese Technological Innovation
- Restricting U.S. Outbound Investment to Targeted Chinese Sectors
- Addressing China's Oppression of Uyghurs
- Exporting Censorship: The Chinese Communist Party Tries to Control Speech About China
- Responding to China at the United Nations
- Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat

But courage in events, featuring important voices, and putting out publications, simply isn't enough. We need to ensure that our effort responds to the very type of lawfare that the CCP has decided to employ. To better assess how the PRC thinks about these issues, it is important to understand that the CCP's effort to use legal systems, the law, and its economic power to its advantage, begins at home, starting with its effort replacing the Western concept of "rule of law" with the more appropriately translated phrase "rule by law."³⁷ This notion, while seeking to hide in terms that American and other Western audiences might relate to, on its face actually seeks to

³⁶ See, e.g., Ben Church, et al., *Houston Rockets GM Daryl Morey, Who Sparked Controversy Between the NBA and China, to Step Down*, CNN (Oct. 16, 2020), available online at <<https://edition.cnn.com/2020/10/16/sport/daryl-morey-nba-china-rockets-stepping-down-spt-intl/index.html>>; Sopan Deb, *Basketball Skills Got Him to the N.B.A., but Activism Made His Name*, N.Y. Times (Mar. 24, 2022), available online at <<https://www.nytimes.com/2022/03/24/sports/basketball/enes-kanter-freedom-nba-activism.html>>.

³⁷ See Jordan Link, et al., *Beijing's Strategy for Asserting Its "Party Rule by Law" Abroad*, Special Report No. 512, United States Institute of Peace (Sept. 2022), at 4, available online at <https://www.usip.org/sites/default/files/2022-09/sr-512_beijing-strategy-for-asserting-party-rule-by-law-abroad.pdf>.

structure a legal system that benefits the CCP internally within China and the PRC externally against the United States and our allies. Internally, what this essentially means is creation of “a system in which the CCP uses the law as a tool to ensure party control of Chinese society while the CCP itself is not bound by that same law,” and in doing so, “outlaws...fundamental freedoms, such as freedom of speech, assembly, and privacy...appl[ying] laws unequally across ethnic, gender, and political spectrums, all in the interest of protecting party control.”³⁸ And externally, this means exporting this construct not just by applying China’s law extraterritorially, by also exploiting existing legal regimes in countries abroad, and even more troublingly, by seeking to shape new law in the CCP’s image.

This first construct, the application of China’s law externally can be seen in examples like the Anti-Foreign Sanctions Law (AFSL), enacted in 2021, which not only “allows the CCP...to retaliate against foreign sanctions but to take measures against any foreign action it perceives as a threat,”³⁹ including by denying visas, seizing the property, or blocking commercial transactions with those individuals or entities that are “involved in designing or implementing the U.S. and EU sanctions” and making such sanctions decisions effectively unreviewable.⁴⁰ Likewise, the CCP uses tools like the “Hong Kong National Security Law and various laws governing technology and trade” to restrict speech and counter what it perceives as “American legal hegemony by replicating US—and sometimes European—laws with expansive extra- territorial applications.”⁴¹ Indeed, in an essay published in the People’s Daily in June 2023, Chinese Foreign Minister Wang Yi explained that China’s then-recently enacted Foreign Relations Law was specifically aimed at responding to what the CCP sees as “hegemonism and power politics” and “counteract[ing] restrictive legal provisions of foreign interference, sanctions, and sabotage against our country.” Indeed, Wang Yi specifically described legislation like the Foreign Relations Law as “a weapon” and argued for the need to further “improv[e] the [PRC’s] legal ‘toolbox’ for foreign struggles.”⁴²

This mirrors language used by Chinese President Xi Jinping back in 2018, where he described the need for China, “[i]n external struggles[,]” to “take up legal weapons.”⁴³ And while we’ve already discussed the PRC’s exploitation of domestic legal systems above as just such a “weapon” to serve the CCP’s interests, it is worth also noting that Xi went further in his 2018 speech, not simply content to focus on how Chinese law ought apply extraterritorially or exploiting existing regimes, but actually making the case for China to seek control of the “rule of law” system built by the Western powers and to actually shape the system in China’s interests by “actively participat[ing]

³⁸ See *id.* at 7.

³⁹ *Id.* at 3.

⁴⁰ See, e.g., Emily Feng, *China's New Anti-Foreign Sanctions Law Sends A Chill Through The Business Community*, National Public Radio (June 11, 2021), available online at <<https://www.npr.org/2021/06/11/1005467033/chinas-new-anti-foreign-sanctions-law-sends-a-chill-through-the-business-communi>>.

⁴¹ See Link, *et al.*, *Beijing’s Strategy*, *supra* n. 31 at 3.

⁴² See John Pomfret, *et al.*, *Capital Markets with Chinese Characteristics*, Foundation for Defense of Democracies (Sept. 14, 2023), available online at <<https://www.fdd.org/analysis/2023/09/14/capital-markets-with-chinese-characteristics/>>.

⁴³ See Xi Jinping, *Strengthen the Party’s Leadership in the Comprehensive Rule of Law*, Inaugural Meeting of the Central Committee for the Comprehensive Rule of Law (Aug. 24, 2018), available online at <<https://interpret.csis.org/translations/strengthen-the-partys-leadership-in-the-comprehensive-rule-of-law-2/>>.

in the formulation of international rules and be a participant, promoter, and leader in the process of global governance reform.”⁴⁴

V. Potential Responses to Consider in Addressing the Threats Posed By China’s Exploitation of Our Legal System.

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

1. **Clear Disclosure Rules in U.S. Courts.** Congress ought consider requiring significant foreign funders of litigation in U.S. courts, whether governments, companies, or individuals, to disclose their role in such litigation and further, ought require any foreign parties to litigation or funders of litigation to fully disclose their ties to foreign governments. Specifically, when it comes to China, such a provision ought require parties to disclose whether: (i) any members of the CCP are in positions of leadership in the organization and what, if any, role they play in corporate decision-making; (ii) the nature and extent of CCP influence in corporate decision making; (iii) any legal requirements on the organization to comply with domestic laws that would require the provision of information on Americans, American companies, or those of our allies to the PRC government; and (iv) the disclosure the total amount and nature of government funding received by the organization in the prior ten years. If it is determined that a foreign funder or party has not met their disclosure obligations, the other party ought be able to seek prompt dismissal of the action.
2. **Heighted Pleading Requirements, Burden Shifting, or Penalty Provisions for Unsuccessful Suits.** Congress ought consider requiring foreign litigants in the U.S. courts to meet a heightened pleading requirement akin to the requirements for pleading fraud, which would make such cases easier to dismiss for American litigants and limit their involvement in the earlier (and costly) stages of litigation, including extensive discovery. Such a requirement might be particularly helpful where foreign entities are targeting individual Americans, particularly researchers, scholars, and activists. Congress might also consider shifting or increasing the burdens of proof to put more requirements on foreign litigants in U.S. courts. Congress might also put in place an attorney fees provision or damages recovery mechanism (perhaps including treble damages) for Americans to utilize against any foreign litigants whose lawsuit fails; this would be particularly ideal where there is a significant disparity in resources between the foreign party and the American party.
3. **Incentivize and Protect Researchers, Scholars, and Activists.** To get ahead of potential threats posed by foreign actors, the U.S. government ought provide incentives to researchers, scholars, and activists who help the U.S. government identify such threats. For example, if such a person identifies a Chinese military-related company or a company violating U.S. sanctions policies, and such identification results in the company being put on the DOD 1260H list or being sanctioned, then the government could provide that individual with a cash bonus coming out of the funds obtained through such sanctions, for

⁴⁴ *Id*

example. In such a scenario, Congress might also consider permitting attorney's fees to be awarded as well to get the trial bar involved in bringing litigation against adversary nations and their proxies. Likewise, the government might consider providing liability protection for individuals whose information led to the government taking some action or even the ability to dismiss the case with prejudice if the individual can prove that their information provided the basis for the government action or if the government provides a letter indicating that such assistance was of use to the government. On a more aggressive note, Congress might consider permitting private rights of action or creating a private attorneys general mechanism or allowing the use of a qui tam construct that enables private actors to sit in the role of the government when, for example, they identify an entity or organization violating U.S. law.

4. **Alternative Discovery and Evidentiary Regimes.** Given that many Chinese companies have close ties to the PRC government and the CCP, it may be difficult to prove certain key jurisdictional facts about a given company. As such, it may be worth Congress considering whether the use of certain types of extrinsic evidence might be permitted or whether appropriate presumptions ought to be applied to foreign litigants with respect to their potential ties to nation-states like China. Congress also might consider whether allowing American litigants broader access to early discovery solely for the purpose of determining whether certain heightened pleading standards or presumptions ought to be applied to a foreign litigant.
5. **Insurance Incentives.** Congress ought consider whether there might be a set of incentives or backstops for reinsurance that could be provided to insurers that would encourage them to provide coverage for individual researchers, scholars, and activists who are seeking to identify potential threats to the nation.
6. **International Rule-Making and Standard Setting.** Given China's clear interest in shaping the existing legal system to its benefit, Congress also ought provide clear direction and funding to the government for both the Executive Branch and private sector to be significantly more engaged in international rule-making and standard setting bodies. Likewise, when engaged in those our other international institutions like the United Nations, is important that the United States and our allies not cave in to pressure from the global repressor nations. So, for example, where we have long proposed our own construct for an international cybercrime treaty and have opposed the construct proposed principally by Russia and China, we ought not at the eleventh hour, change our perspective on such a treaty and support it in Committee as happened recently.

VI. Conclusion

For nearly a decade now, China has telegraphed that it intends to use our legal system and our conception of the rule of law against us, including against our own companies, our people, and our nation. China has likewise made clear that it will close off its system to us and that our companies and people will have limited, if any, recourse in China's legal system. We now need to recognize these actions for what they are, namely a full-scale attempt to undermine the core rule of law and bend it to the CCPs favor. Given this, we ought take swift action to halt this move and to reset or

modify the rules in our system to protect and defend the values we hold near and dear and to incentivize those who engage in them. At the core of these values are those of freedom of inquiry and free speech, values that have long enabled American researchers, scholars, and activists the ability to call out those who act badly across the globe with relative impunity.

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, Ashutosh Bhagwat, Stuart N. Brotman, Anupam Chander, Erwin Chemerinsky, James Grimmelman, 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 Contents.....	iv
Table of Authorities	v
Glossary	xiii
Interest of Amici Curiae.....	xiv
Summary of Argument.....	1
Argument	3
I. The Chinese government’s control of TikTok presents a novel and serious national security threat.....	3
II. The Act is a measured step to resolve the national security concerns posed by the Chinese government’s control of TikTok.	14
A. The political branches have flagged the national security concerns posed by Chinese control of TikTok.....	14
B. TikTok has failed to respond to these legitimate concerns.....	21
C. Project Texas does not mitigate the risks or address the ongoing harms.....	23
D. Congress passed the Act to resolve the national security concerns posed by Chinese control of TikTok.	25
III. The government’s compelling national security interests overcome any applicable level of First Amendment scrutiny.....	26
Conclusion.....	33
Certificate of Compliance	34
Appendix A: List of Amici Curiae

TABLE OF AUTHORITIES

Cases

<i>Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.</i> , 591 U.S. 430 (2020)	28
<i>Broadrick v. Oklahoma</i> , 413 U.S. 601 (1973)	29
<i>China Telecom (Americas) Corp. v. FCC</i> , 57 F.4th 256 (D.C. Cir. 2022)	27
<i>Haig v. Agee</i> , 454 U.S. 280 (1981)	28, 33
<i>Hamdi v. Rumsfeld</i> , 542 U.S. 507 (2004)	14
<i>Heart of Atlanta Motel, Inc. v. United States</i> , 379 U.S. 241 (1964)	14
<i>Heffron v. International Soc'y for Krishna Consciousness, Inc.</i> , 452 U.S. 640 (1981)	30, 32
<i>Kovacs v. Cooper</i> , 336 U.S. 77 (1949)	30
<i>Murthy v. Missouri</i> , 144 S. Ct. 1972 (2024)	29
<i>Pacific Networks Corp. v. FCC</i> , 77 F.4th 1160 (D.C. Cir. 2023)	27
<i>Sorrell v. IMS Health, Inc.</i> , 564 U.S. 552 (2011)	28
<i>TikTok Inc. v. CFIUS</i> , No. 20-1444 (D.C. Cir. 2020)	17
<i>United States v. Curtiss-Wright Export Corp.</i> , 299 U.S. 304 (1936).	31
<i>United States v. O'Brien</i> , 391 U.S. 367 (1968)	31, 32
<i>United States v. Zhiyong</i> , 1:20-cr-00046 (N.D. Ga. Jan. 28, 2020)	9

<i>Ward v. Rock Against Racism</i> , 491 U.S. 781 (1989)	30
<i>Zivotofsky ex rel. Zivotofsky v. Kerry</i> , 576 U.S. 1 (2015)	31
Statutes	
12 U.S.C. §72	26
16 U.S.C. §797	26
42 U.S.C. §§2131-34.....	26
47 U.S.C. § 310(b)(3).....	27
49 U.S.C. §§ 40102.....	27
Pub. L. No. 117-328, div. R (2023)	16
Pub. L. No. 118-50, div. H (2024).....	25, 26
Regulations	
<i>Addressing the Threat Posed by TikTok</i> , 85 Fed. Reg. 48637-38 (Aug. 6, 2020)	15
<i>Preventing Access to American’s Bulk Sensitive Personal Data</i> , 89 Fed. Reg. 15780 (Feb. 28, 2024)	16
<i>Protecting Americans’ Sensitive Data from Foreign Adversaries</i> , 86 Fed. Reg. 31423 (June 9, 2021)	15
<i>Statement by Secretary Steven T. Mnuchin Regarding the Acquisition of Musical.ly by ByteDance Ltd.</i> , 85 Fed. Reg. 51297, 51297 (Aug. 14, 2020)	15
Executive Branch Sources	
<i>Attorney General William P. Barr Announces Indictment of Four Members of China’s Military for Hacking into Equifax</i> , Dep’t of Justice (Feb. 10, 2020), https://perma.cc/9GRX-QR4V	8
<i>Chinese Military Hackers Charged in Equifax Breach</i> , Federal Bureau of Investigation (Feb. 10, 2020) https://perma.cc/7JPH-G2EC	7, 8
<i>Fireside Chat with DNI Haines</i> , DNI Office (Dec. 3, 2022), https://perma.cc/L6AY-TL4D	17

<i>Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions</i> , Dep’t of Justice (May 9, 2019) https://perma.cc/77P4-T7Y5	7, 8
Memorandum for the Heads of Executive Departments and Agencies, “ <i>No TikTok on Government Devices</i> ” Implementation Guidance, OMB M-23-13 (Feb. 27, 2023).....	16
<i>President’s Decision Regarding the Acquisition by ByteDance Ltd. of the U.S. Business of muical.ly</i> , U.S. Dep’t of Treasury (Aug. 14, 2020)....	14
<i>Press Gaggle by Principal Deputy Press Secretary Olivia Dalton</i> , White House Briefing Room (Feb. 28, 2023) https://perma.cc/92PD-SQ66	16
<i>Remarks by President Biden Before Air Force One Departure</i> , White House Briefing Room (Mar. 8, 2024) https://perma.cc/58NG-4YAP	16
<i>Safeguarding Our Future</i> , The National Counterintelligence and Security Center https://perma.cc/549G-W4X2	4
Congressional Sources	
H.R. 815, 118th Cong., Congress.gov (Apr. 24, 2024).....	25
<i>Hearing Memorandum</i> , H. Comm. on Energy & Commerce, No. 118-13, 118th Cong., 1st Sess. (Mar. 20, 2023)	19
<i>Hearing on 2024 Annual Threat Assessment</i> , U.S. Senate Select Committee Intelligence Hearing (Mar. 11, 2024)	4
<i>Hearing on Oversight of the Federal Bureau of Investigation</i> , House Judiciary Committee (July 12, 2023)	5
<i>Hearing on the 2023 Annual Threat Assessment of the U.S. Intelligence Community</i> , U.S. Senate Select Comm. Intelligence Hearing (Mar. 8, 2023).....	2
<i>Letter from Rep. Mike Gallagher to Christopher Wray, FBI Director</i> (Dec. 7, 2023)	4, 20
<i>Letter from TikTok Inc. to Senators Blumenthal and Blackburn</i> (June 16, 2023).....	18

<i>Press Conference to Introduce the Protecting Americans from Foreign Adversary Controlled Applications Act</i> , China Select Committee (Mar. 6, 2024).....	20
Press Release, <i>Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans from Foreign Adversary Controlled Applications, Including TikTok</i> (Mar. 5, 2024).....	19, 25
Press Release, <i>Senators Introduce Bipartisan Bill to tackle National Security Threats from Foreign Tech</i> (Mar. 7, 2023).....	18
<i>Protecting Americans from Foreign Adversary Controlled Applications</i> , H. Rep. 118-417, 118th Cong., 2d Sess. 1 (Mar. 11, 2024).....	19
<i>Restricting TikTok (Part I): Legal History & Background</i> , LSB10940 (Updated Sept. 28, 2023).....	19
<i>Restricting TikTok (Part II): Legislative Proposals & Considerations for Congress</i> , LSB10942 (updated Mar. 15, 2024).....	19
Roll Call 145: H.R. 8038, Clerk of the United States House of Representatives, 118th Cong.(Apr. 20, 2024).....	25
Roll Call 154: H.R. 815, United States Senate, 118th Cong. (Apr. 23, 2024)	25
<i>Testimony of Shou Chew</i> , H. Comm. on Energy & Commerce, No. 118-13, 118th Cong., 1st Sess. (Mar. 23, 2023)	19
<i>The Select: ‘TikTok Special’-A weekly Committee Recap</i> (Mar. 8, 2024).....	3, 10, 13
<i>TikTok: Frequently Asked Questions & Issues for Congress</i> , R48023 (Apr. 9, 2024), https://perma.cc/U2Q8-3L3N	19
<i>TikTok: How Congress Can Safeguard American Data Privacy</i> , Hearing Before the H. Comm. on Energy & Commerce, 118th Cong. (2023).....	7, 19, 21
<i>TikTok: Recent Data Privacy & Nat’l Security Concerns</i> , IN12131 (Mar. 29, 2023).....	19
<i>TikTok: Technology Overview & Issues</i> , R46543 (updated June 30, 2023)	19

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)..... 18

News Sources

Alexander Ward & Matt Berg, *Why bin Laden’s letter went viral on social media*, Politico (Nov. 16, 2023)
<https://perma.cc/4FSS-QYEW> 13

Bethany Allen-Ebrahimian, *FCC commissioner says government should ban TikTok*, Axios (Nov. 1, 2022)
<https://perma.cc/WA2Y-XA76>..... 18

Cecelia Smith-Schoenwalder, *5 Threats FBI Director Wray Warns the U.S. Should Be Worried About*, U.S. News (Jan. 31, 2024)
<https://perma.cc/D3B6-Y3UR>..... 17

D. Harwell & T. Room, *Inside TikTok*, Washington Post (Nov. 5, 2019),
<https://perma.cc/B368-JNN4> 23

D. Wallace, *TikTok CEO grilled on Chinese Communist Party influence*, Fox Business (Jan. 31, 2024),
<https://perma.cc/KJ9F-8HJ7> 22

Dan Verton, *Impact of OPM breach could last more than 40 years*, FEDSCOOP (July 10, 2015),
<https://perma.cc/E6QH-JHLU>..... 10

Deputy attorney general warns against using TikTok, citing data privacy, ABCNews (Feb. 16, 2023),
perma.cc/GKK7-BX9D..... 18

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> 12

Emily Baker-White, *EXCLUSIVE: TikTok Spied on Forbes Journalists*, Forbes (Dec. 22, 2022),
<https://perma.cc/XUS8-ATNP> 7

Emily Baker-White, *TikTok’s Secret ‘Heating’ Button Can Make Anyone Go Viral*, Forbes (Jan. 20, 2023),
<https://perma.cc/RW78-KTV9> 11

<i>FBI Chief Says TikTok ‘Screams’ of US National Security Concerns</i> , Reuters (Mar. 9, 2023), https://perma.cc/F5WC-7AF3	17
Gaby Del Valle, <i>Report: TikTok’s effort to silo US data ‘largely cosmetic’</i> , The Verge (Apr. 16, 2024), https://perma.cc/WR45-NZCU	24
Georgia Wells, <i>TikTok Struggles to Protect U.S. Data from Its China Parent</i> , WSJ (Jan. 30, 2024), https://archive.is/a8LtA	24
<i>Homeland Security Secretary on TikTok’s Security Threat</i> , Bloomberg (May 29, 2024), https://perma.cc/W7PQ-68XH	17
<i>House lawmakers deeply concerned over TikTok despite CEO’s testimony</i> , CBS News (Mar. 23, 2023), https://perma.cc/H95J-PETG	3
Ken Tran & Rachel Looker, <i>What does TikTok do with your data?</i> , USA Today (Mar. 23, 2023), https://perma.cc/2LVQ-3Z6L	22
Kevin Breuninger & Eamon Javers, <i>Communist Party cells influencing U.S. companies’ China operations</i> , CNBC (July 12, 2023), https://perma.cc/TU6B-GHYV	5
Lauren Feiner, <i>TikTok CEO says China-based ByteDance employees still have access to some U.S. data</i> , CNBC (Mar. 23, 2023), https://perma.cc/9LU9-JBAN	22
Louis Casiano & Hillary Vaughn, <i>TikTok CEO refuses to answer if Chinese government has influence over platform as Congress mulls ban</i> , Fox Business (Mar. 14, 2024), https://perma.cc/8BCT-ERTL	22
Sapna Maheshwari & David McCabe, <i>TikTok Prompts Users to call Congress to Fight Possible Ban</i> , N.Y. Times (Mar. 7, 2024), https://perma.cc/GD3J-QNPV	2, 11
See Emily Baker-White, <i>Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed</i>	

<i>From China</i> , BuzzFeed (June 17, 2022), https://perma.cc/7LF4-Y3XD	24
Thomas Fuller & Sapna Maheshwari, <i>Ex-ByteDance Executive Accuses Company of ‘Lawlessness,’</i> N.Y. Times (May 12, 2023), perma.cc/DE96-KD7G	6
<i>US House passes bill that would ban TikTok</i> , Live Now Fox (Mar. 13, 2024) https://perma.cc/9M77-TQNW	9
Yaqiu Wang, <i>The Problem with TikTok’s Claim of Independence from Beijing</i> , The Hill (Mar. 24, 2023), https://perma.cc/L44R-U9HL	6
Zen Soo, <i>Former ByteDance executive says Chinese Communist Party tracked Hong Kong protesters via data</i> , AP News (June 7, 2023), https://perma.cc/K9HB-XDBL	6, 7
Other Authorities	
<i>A Tik-Tok-ing Timebomb</i> , NCRI and Rutgers Miller Center (Dec. 2023), https://perma.cc/4RFG-69RE	12
<i>A Tik-Tok-ing Timebomb: How TikTok’s Global Platform Anomalies Align with the Chinese Communist Party’s Geostrategic Objectives</i> , NCRI and Rutgers Miller Center (Dec. 2023), https://perma.cc/4RFG-69RE	29
Fergus Ryan, et al., <i>TikTok and WeChat: Curating and controlling global information flows</i> , Australian Strategic Policy Institute (2020), https://perma.cc/K3SF-DH2H	29
Fergus Ryan, et al., <i>TikTok and WeChat: Curating and Controlling Global Information Flows</i> , Australian Strategic Policy Institute (2020), https://perma.cc/K3SF-DH2H	12
Lauren Yu-Hsin Lin & Curtis J. Milhaupt, <i>CCP Influence over China’s Corporate Governance</i> , Stanford Ctr. on China’s Economy and Institutions (updated Nov. 1, 2022) https://perma.cc/PYL3-DDN2	5
<i>Privacy Policy</i> , TikTok (last updated July 1, 2024), https://perma.cc/RV8S-U38H	3

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>..... 13

Scott Livingston, *The New Challenge of Communist Corporate Governance*, Ctr. for Strategic & Int’l Studies (Jan. 2021),
<https://perma.cc/X3KY-AYLC> 5

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 listen 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 musical.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 Vaughn, *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 bipartisan 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 *anyone 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 divestiture—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 Geostategic 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 Counterterrorism 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