Nos. 24-656, 24-657

IN THE
Supreme Court of the United States

TIKTOK INC. AND BYTEDANCE LTD.,
Petitioners,
v.
MERRICK B. GARLAND, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES,
Respondent.

BRIAN FIREBAUGH, ET AL.,
Petitioner,
v.
MERRICK B. GARLAND, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES,
Respondent.

On Writs of Certiorari to the United States Court of Appeals for the D.C. Circuit

BRIEF OF *AMICI CURIAE* FORMER NATIONAL SECURITY OFFICIALS IN SUPPORT OF RESPONDENT

THOMAS R. MCCARTHY
KATHLEEN S. LANE
Counsel of Record
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com
katie@consovoymccarthy.com

Counsel for Amici Curiae

December 27, 2024

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

INTEREST OF *AMICI CURIAE*[1]

Amici curiae[2] are former national security government officials in their individual capacities. Amici file 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 to America's national security. TikTok presents one such critical foreign national security 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.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

Approximately 170 million Americans use TikTok. *TikTok Inc. v. Garland*, ---F.4th ---, 2024 WL 4996719, at *2 (D.C. Cir. Dec. 6, 2024). Like other social media applications, TikTok collects massive amounts of personal data on its users, and TikTok has a proprietary

---

[1] Pursuant to this Court's Rule 37.6, counsel for *amici curiae* certifies that this brief was not authored in whole or in part by counsel for any party and that no person or entity other than *amici curiae* or its counsel has made a monetary contribution to the preparation or submission of this brief.

[2] For a full list of amici curiae, see Appendix 1a.

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 ("CCP"). Congress, recognizing the national security threat posed by CCP's control over TikTok, sought to address this threat by enacting the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 955 (Apr. 24, 2024) (the "Act").

TikTok is owned by a Chinese company beholden to the Chinese Communist Party. Chinese government control over TikTok both affords the CCP direct access to the massive amounts of sensitive personal data of TikTok's 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 these vast swaths of personal information for its own benefit and to the detriment of the United States and our national security. As Senator Rubio 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) (statement of Senator Rubio) ("*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 on behalf of a foreign government. Indeed, in one stark example, in the lead up to the enactment of the statute at issue in this matter, 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/9AHY-7Z8X.

Following enactment of the Act, TikTok and others challenged the Act in court. After reviewing the record in full, the D.C. Circuit confirmed what Congress had already identified to be true: TikTok poses a serious national security threat to the United States and its citizens. *TikTok*, 2024 WL 4996719, at *13. Indeed, the D.C. Circuit concluded that the Act survives any level of First Amendment scrutiny precisely because of these national security concerns. *Id.* at *12.

Amici agree with the D.C. Circuit that the Act is a lawful exercise of Congressional authority, consistent with the First Amendment and other constitutional concerns. Amici write separately to emphasize the serious national security threats posed by the CCP's control of TikTok; to argue that the First Amendment does not apply to a foreign adversary's collection of data and manipulation of social media algorithims to convey its preferred messaging; to explain why TikTok's attempts to address the national security concerns have fallen short; and to explain that the compelling national security interests are narrowly tailored to overcome any applicable level of First Amendment scrutiny should it apply to TikTok's activities.

The Supreme Court should affirm.

ARGUMENT

I. The D.C. Circuit correctly concluded that the Chinese government's control of TikTok presents a serious national security threat.

TikTok presents a serious and unique national security threat to the United States because the sensitive personal data it both openly and surreptitiously collects on Americans is made available to the Chinese Communist Party and because TikTok's ability to influence information shared through the application with Americans is subject to the direction and control of the CCP. It is undisputed that TikTok collects massive amounts of sensitive personal information about the 170 million Americans using its application. *TikTok*, 2024 WL 4996719 at *5. By its own admission, the TikTok application 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.

According to the House China Select Committee, TikTok also surreptitiously collects the voice and location data of Americans, even when the user is not using the application and even if the user has set their privacy settings to prohibit the collection of such data. *The Select: 'TikTok Special'-A weekly Committee Recap* (Mar. 8, 2024), https://perma.cc/Z7YH-SW9S. Collectively, this data—from profile details to the content of private messages to individualized voice content and location data—allows the CCP to have massive amounts of sensitive personal information about the 170 million Americans using TikTok's application.

FBI Director Christopher Wray has explained in testimony to Congress that TikTok is owned by ByteDance, a Chinese corporation that the FBI Director describes as being "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. The type of data the TikTok application collects on Americans—both openly as well as surreptitiously—is deeply concerning even absent any connection to a foreign nation-state. However, given the relationship between ByteDance and the CCP, the access to this data that China's National Intelligence Law provides to the CCP makes its collection even more troubling. That law affirmatively *requires* ByteDance and TikTok to assist with intelligence gathering, providing China's intelligence agencies with direct access to the massive troves of sensitive personal data of Americans collected through TikTok. *See Letter from Rep. Mike Gallagher to Christopher Wray, FBI Director*, at 1 (Dec. 7, 2023), https://perma.cc/R352-UFKG; *Safeguarding Our Future*, The National Counterintelligence and Security Center, https://perma.cc/549G-W4X2 (last updated June 20, 2023).

The CCP also exercises significant internal influence over TikTok. The CCP requires certain companies, including ByteDance, to ensure "compliance with [CCP] orthodoxy" by hosting an internal CCP party committee. *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 many Chinese companies, their charters directly incorporate 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.

The CCP's influence over TikTok and ByteDance is apparent and pervasive. Last year, under pressure from the CCP, ByteDance executives publicly apologized for deviating from "socialist core values" for "vulgar" content on one of its other applications. *See Ya-qiu Wang, The Problem with TikTok's Claim of Independence from Beijing*, The Hill (Mar. 24, 2023), https://perma.cc/L44R-U9HL. And ByteDance has known history of using its data collection to track political activity of those the CCP is concerned about, including the 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, *infra*; *TikTok: How Congress Can Safeguard American Data Privacy*, Hearing Before the H. Comm. on Energy & Commerce, 118th Cong. (2023) ("2023 House Data Privacy Hearing"). One former TikTok executive has confirmed publicly 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. *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 CCP's external and internal control over TikTok means that when TikTok collects massive amounts of personal data, including the private conversations and sensitive information of the 170 million Americans on its platform, this data is then directly accessible by the CCP and its intelligence services. Moreover, these 170 million Americans' access to content on the platform is also directed by the CCP, which influences the algorithms used by TikTok and information it conveys to it users. *Id*.

Standing alone, the influence the CCP has over TikTok and ByteDance gives rise to serious national security concerns. But when looking at this influence in conjunction with the other information that the Chinese government has collected through a broad range of cyber hacks targeting both ordinary Americans and U.S. government officials, and extending over more than a decade, the CCP's involvement in TikTok poses an unacceptable national security risk to the United States and its citizens. *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.

For example, in the 2015 OPM breach, Chinese government hackers exfiltrated the security clearance files of over 20 million Americans with Top Secret/ Sensitive Compartmented Information (TS/SCI) clearances. This data included the acquisition, by the CCP, of detailed "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. *See Sanger, supra*. In the 2016 Anthem Healthcare hack, the Chinese government obtained the addresses, birth dates, and social security numbers of more than 78 million Americans and may also have obtained protected health information on these Americans. *See Anthem Breach, supra*. Similarly, in the 2017 Equifax data breach, Chinese military hackers 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 2018 Marriott hack, Chinese hackers working for the Ministry of State Security, 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*. This means that, over the course of the last decade, hackers with direct ties to China and the CCP have compromised hundreds of millions of Americans' sensitive information, including financial, healthcare, travel, and personal relationship information.

It is difficult to overstate the national security impact of these hacks, especially when reviewed in context of TikTok's constant monitoring and data collection on 170 million Americans. Through TikTok, the Chinese government has access to information about these Americans' day-to-day routines. They know who these Americans interact with, what they do, where they go, and what they say to others on the platform (and perhaps off it, with the TikTok app's surreptitious collection of voice content). And because of their other hacks, the Chinese government now has access to these individuals' most sensitive personal information that they can combine with TikTok's data.

The CCP can exploit this massive trove of sensitive data—the TikTok data combined with data collected from other hacks—to power sophisticated artificial intelligence (AI) capabilities that can then be used to identify specific 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.

Beyond using TikTok for massive data collection, the CCP also uses TikTok to influence Americans by pushing specific CCP-chosen content while hiding its source. Americans use TikTok for much more than just watching or promoting "weird dance videos." *The Select: 'TikTok Special,' supra* (statement of Chairman Gallagher). Indeed, many Americans—particularly, younger Americans—use the application as their primary news source. *Id.* (describing TikTok as the "dominant news platform for Americans under 30"). Given the CCP's external and internal influence over ByteDance and TikTok, this reliance by young people on TikTok for their daily news feed ensures that the CCP maintains editorial control over the content that tens of millions of young Americans consume every single day.

TikTok and ByteDance also have the power to boost (or de-emphasize) certain videos and themes through their proprietary and confidential recommendation algorithm, thus providing CCP officials yet another tool 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, in the lead up to the passage of the legislation now before this Court, TikTok sent 170 million Americans a message encouraging them to call their representatives in Congress and oppose it. Maheshwari & McCabe, *supra*. This lobbying effort—created and driven by ByteDance, a foreign nation-state proxy—prompted a "flood of phone calls" to congressional offices to oppose a purported "TikTok shutdown." *Id.*

Likewise, the CCP has quickly and effectively deployed TikTok to spread misinformation and promote propaganda to influence important American policy debates about our own national security and that of our allies. For example, in November 2023, after the horrific October 7 terrorist attacks conducted by Hamas in Israel, videos praising Osama bin Laden's 2002 "Letter to America" were promoted across American's TikTok feeds. *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. Lawmakers questioned whether TikTok—controlled by the CCP—was affirmatively boosting the video, but were unable to verify whether the TikTok algorithm was responsible. And the reason for their inability to make this determination is because, perhaps unsurprisingly, the CCP (and ByteDance), have consistently refused to share any information on how content is promoted (or demoted) on TikTok. Alexander Ward & Matt Berg, *Why bin Laden's letter went viral on social media*, Politico (Nov. 16, 2023), https://perma.cc/4FSS-QYEW. Moreover, even if TikTok itself did not affirmatively boost these videos, it is clear that TikTok can serve a "force multiplier," for CCP-directed misinformation, with researchers finding that "[w]ith more than two billion TikTok users, a strategically crafted misinformation campaign can have a high chance of success," and noting the "potential for [such videos]…to be[] a severe national security threat…[with] 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.

Lest this concern seem hypothetical, it is worth noting that TikTok has already utilized its algorithm

to suppress content that is adverse to the interests of the CCP. In 2023, for example, the Network Contagion Research Institute (NCRI) found that the TikTok recommendation algorithm regularly down-prioritized content critical of the Chinese regime or supportive of Hong Kong democracy 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.

At the same time, TikTok's algorithm can boost users' perception of China itself. Access to data collected by TikTok about Americans, when combined with the ability to shape what the TikTok platform provides to Americans creates a powerful tool for CCP manipulation, the dangers of which must be understood in the context of well-established CCP policy and strategy. Scholars have highlighted that "[s]ince 2020, government organs [in China] have carried out waves of private regulation to discipline companies, align their actions with party priorities, [and] strengthen party influence" over the private sector. *See* Katja Drinhausen & Helena Legarda, *Confident Paranoia: Xi's 'comprehensive national security' framework shapes China's behavior at home and abroad,* Merics China Monitor, at 14 (Sept. 15, 2022), https://perma.cc/ZFW4-HVAT. And these same scholars have noted that while "China's national security state once largely remained within China's borders…[it] is [now] expanding internationally...and efforts to control China-related narratives and policies internationally are meant to help Beijing achieve [its] goals." *Id*. at 15. In this context, TikTok's ability to shape what millions of young Americans see, hear, and—eventually, the CCP

hopes—think about China likewise makes the TikTok platform a national security threat to the United States.

The use of TikTok to gather massive amounts of information in combination with the fruits of coordinated cyber hacks to enable even more sophisticated intelligence collection against Americans, as well as the internal pressure and control over company policy resulting in coordinated propaganda pushed by TikTok, taken together, "pos[e] a clear and present threat to America." *The Select: 'TikTok Special,' supra*.

II. The Act targets and resolves the national-security threat posed by the Chinese government's control of TikTok.

The United States appropriately offers two key national security justifications for the Act. First, the Act counters the CCP's efforts to collect information about individuals in the United States. *TikTok*, 2024 WL 4996719, at *13. And second, the Act addresses the risk of the CCP's manipulation of content on TikTok. The D.C. Circuit correctly concluded that each of these justifications "constitutes an independently compelling national security interest." *Id.*

A. The political branches repeatedly and consistently have highlighted and acted to address the national security concerns supporting the Act.

The D.C. Circuit correctly recognized that the "multi-year efforts of both political branches" and the "bipartisan action by the Congress and by successive presidents" weighed "heavily in favor of the Act." *TikTok*, 2024 WL 4996719, at *13.

The Executive Branch has been sounding the alarm over TikTok for years. In 2019, the Committee on

Foreign Investment in the United States (CFIUS) initiated a review of ByteDance's acquisition of musical.ly, citing national security concerns. *President's Decision Regarding the Acquisition by ByteDance Ltd. of the U.S. Business of muical.ly*, U.S. Dep't of Treasury (Aug. 14, 2020); *see also TikTok*, 2024 WL 4996719, at *3. Following that review, 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). President Trump also separately invoked his powers under the International Emergency Economic Powers Act and the National Emergencies Act to address the threat of TikTok, which the President noted "allow[s] the Chinese Communist Party access to Americans' personal and proprietary information." *Addressing the Threat Posed by TikTok*, 85 Fed. Reg. 48637-38 (Aug. 6, 2020); *see also TikTok*, 2024 WL 4996719, at *4. President Trump also revealed that TikTok's data collection included information about "the locations of Federal employees and contractors" and noted that its continued collection of data on individual Americans would give China the capability to "build dossiers of personal information for blackmail, and conduct corporate espionage." 85 Fed. Reg. at 48637.

Although President Biden formally revoked President Trump's order, he continued to highlight TikTok's problematic data collection and the resulting national-security risks and took further action to curtail foreign adversaries' access to sensitive data on Americans. *See Protecting Americans' Sensitive Data from Foreign Adversaries*, 86 Fed. Reg. 31423 (June 9, 2021). And after Congress prohibited the use of TikTok on

government devices, the White House moved quickly to implement 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, 136 Stat. 5258 (Dec. 29, 2022). 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. President Biden later confirmed he would support legislation banning TikTok altogether. *Remarks by President Biden Before Air Force One Departure*, White House Briefing Room (Mar. 8, 2024), https://perma.cc/58NG-4YAP. In particular, the Biden Administration specifically acknowledged that data collection by "countries of concern," like China, raises the risk of "malicious activities" like "espionage, influence, kinetic, or cyber operations." *See Preventing Access to American's Bulk Sensitive Personal Data*, 89 Fed. Reg. 15780, 15781 (Feb. 28, 2024).

In addition to presidential acts and public statements, numerous senior Executive Branch officials have also warned the American public and Congress about the national security threats posed by TikTok. *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.[3] As the D.C. Circuit noted, the judgment

[3] *See, e.g.*, *FBI Chief Says TikTok 'Screams' of US National Security Concerns*, Reuters (Mar. 9, 2023), https://perma.cc/F5

of the Executive Branch regarding this national security threat "'is entitled to significant weight, and we have persuasive evidence [in the public record] before us to sustain it.'" *TikTok*, 2024 WL 4996719, at *15 (quoting *Holder v. Humanitarian Law Project*, 561 U.S. 1, 36 (2010)).

Likewise, bipartisan coalitions in Congress have sought to address the concerns over TikTok's data collection practices.[4] On the Senate side, then-Senate Intelligence Committee Chairman Mark Warner (D-VA) and then-Minority Whip (and now incoming Majority Leader) Senator John 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. On the House side, then-House China Select Committee Chairman Mike Gallagher (R-WI) and Ranking Member Raja Krishnamoorthi (D-IL) stated that "[s]o long as [TikTok] is owned by ByteDance…TikTok poses critical threats to our national security." Press Release, *Gallagher, Bipartisan Coalition Introduce Legislation*

WC-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.

[4] *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.

to Protect Americans from Foreign Adversary Controlled Applications, Including TikTok (Mar. 5, 2024) ("*Gallagher Press Release*"), https://perma.cc/6NHJ-ZQCJ. Consistent with the concerns raised by senior Members of Congress in both chambers, Congress held several hearings and briefings on critical privacy and security threat posed by TikTok.[5] At one of these hearings, Senator Marco Rubio (then the Vice Chairman of the Senate Intelligence Committee and now the Secretary of State-designate) asserted that TikTok "is probably one of the most valuable surveillance tools on the planet." *2023 Threat Assessment Hearing* at 1:09:00, *supra*.

The House of Representatives was so concerned about the national security threat posed by China that it established a Select Committee to examine the issue and, over the past two years, the Committee has led the effort on Capitol Hill to sound the alarm over the national security threat posed by China and the CCP, including the specific 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*

---

[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.

Controlled Applications Act, China Select Committee (Mar. 6, 2024) (statement of Chairman Gallagher), https://perma.cc/NBC3-H3PB.[6] At another hearing, former CIA Director and Secretary of State Mike Pompeo stated that TikTok is 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 failed to respond to these concerns.

Even though both the Executive Branch and Congress repeatedly have raised concerns over TikTok, TikTok has failed to effectively address these concerns or

---

[6] The federal government is not alone in its concern about TikTok. The States have launched several bipartisan investigations into different parts of the application, whether it be data collection, child protection, police powers, or general sovereign authority over businesses operating within their borders. *See, e.g.*, David Shepardson, *State AGs demand TikTok comply with US consumer protection 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. As of March 2024, thirty-nine States have barred TikTok from state 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.

otherwise answer legitimate questions about its data collection and storage practices. *See 2023 House Data Privacy Hearing*, *supra*.

At a congressional hearing in 2023, TikTok's CEO confirmed that China-based employees have access to sensitive personal U.S. data and refused to answer whether the Chinese government exerts influence over TikTok. *See* 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; Louis Casiano & Hillary Vaugh, *TikTok CEO refuses to answer if Chinese government has influence over platform as Congress mulls ban*, Fox Business (Mar. 14, 2024), https://perma.cc/8BCT-ERTL; Ken Tran & Rachel Looker, *What does TikTok do with your data?*, USA Today (Mar. 23, 2023), https://perma.cc/2LVQ-3Z6L. When pressed about the Chinese government's influence, the CEO of TikTok simply stated that "all businesses that operate in China have to follow the law," effectively skirting the question while also tacitly acknowledging what the political branches have raised as a core concern about TikTok: that China's own laws and CCP policies essentially make it a wholly-owned and operated subsidiary of the CCP and the Chinese government. *See* D. Wallace, *TikTok CEO grilled on Chinese Communist Party influence*, Fox Business (Jan. 31, 2024), https://perma.cc/KJ9F-8HJ7.

TikTok ostensibly has sought to mollify the federal government's concerns by creating Project Texas, which it claims would ensure that the massive trove of sensitive data it collects on its 170 million American users would be retained wholly in the United States. But Project Texas has failed to eliminate key national security concerns because TikTok's own public statements

show that the CCP continues to have access to user data stored in the United States. For example, there remain concerns that even under Project Texas, China would continue to have leverage "over the people who have access to [American] data," *see* D. Harwell & T. Room, *Inside TikTok*, Washington Post (Nov. 5, 2019), https://perma.cc/B368-JNN4, and 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, *see* Georgia Wells, *TikTok Struggles to Protect U.S. Data from Its China Parent*, WSJ (Jan. 30, 2024), https://perma.cc/J43J-YBFR.

Given all this, it is clear that Project Texas is a "cosmetic" fix, not a substantive transformation of TikTok's data collection and storage practices. *See* Gaby Del Valle, *Report: TikTok's effort to silo US data 'largely cosmetic'*, The Verge (Apr. 16, 2024), https://perma.cc/WR45-NZCU. Regardless of where TikTok data is stored, the CCP can access the data. *Id.* Indeed, American consultants for Project Texas were caught on leaked recordings admitting that even "with these [Project Texas-approved] tools, there's some backdoor to access user data in almost all of them." *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. In short, Project Texas simply confirms the extent to which TikTok is tied to the CCP and highlights the need for a targeted legislative fix like the Act. That China has stated unequivocally that it will "not permit a forced divestment" of TikTok to an American company only further serves to validate these concerns. TikTok Brief, *TikTok, Inc. v. Garland*, 24-1113, at 2 (June 20, 2024).

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. But the Act doesn't even implicate the First Amendment.

As an initial matter, "foreign persons and corporations located abroad do not … possess First Amendment rights." *Moody v. NetChoice, LLC*, 603 U.S. 707, 746-47 (2024) (Barrett, J., concurring) (citing *Agency for Int'l Devpmt v. All. For Open Soc'y Int'l, Inc.*, 591 U.S. 430, 433-36 (2020)). ByteDance's "foreign ownership and control" over TikTok, including its data collection and content manipulation directed by a foreign government, wholly removes TikTok from the protection of the First Amendment.

Moreover, the Act itself is narrowly tailored to specifically target the CCP's control of TikTok, only requiring divestiture by its Chinese owners if TikTok seeks to continue accessing sensitive personal data of Americans and controlling the algorithms that drive the content viewed by audiences in the United States. The government has long regulated—and prohibited in appropriate cases—foreign ownership and control of companies operating in all sorts of industries, including telecommunications and media. *See, e.g.*, 47 U.S.C. §310(b)(3) (radio and broadcast television); 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).

The Act is no different. It requires divesture of TikTok as a precondition to operating in the United States. As the D.C. Circuit explained, the Act's provisions are "limited to foreign adversary control of a substantial medium of communication and include a divestiture exemption." *TikTok*, 2024 WL 4996719, at *20. Specifically, the court said, the Act targets Chinese "ownership and control" over the application, which is how the federal government has handled similar situations previously. For example, in *Pacific Networks Corp. v. FCC*, the D.C. Circuit similarly 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." *Pacific Networks Corp. v. FCC*, 77 F.4th 1160, 1162-63 (D.C. Cir. 2023); *see also China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 265-66 (D.C. Cir. 2022). And, in this case specifically, it is clear that there are American organizations willing to step up and take ownership of TikTok in a divestment scenario. *TikTok takeover: Here's which billionaires are putting together bids and what they propose for users*, N.Y. Post (Dec. 23, 2024), https://perma.cc/3GHM-AT6L.

But even if this Court agrees with the D.C. Circuit that the First Amendment applies to the Act, the D.C. Circuit correctly recognized that the Act satisfies even strict scrutiny. *TikTok Inc.*, 2024 WL 4996719, at *9. After all, national security is the "principal purpose[]" of the federal government. The Federalist No. 23 (Alexander Hamilton); *see also* Federalist Nos. 34

(Alexander Hamilton), 41 (James Madison). For the reasons explained above, *supra* Sections I and II, the Act "was the culmination of extensive, bipartisan action by the Congress and by successive presidents" and narrowly addressed the "well-substantiated national security threat posed by" the CCP. *TikTok Inc.*, 2024 WL 4996719, at *13. As the D.C. Circuit held, the Act survives any level of First Amendment scrutiny. *Id*. at *9.

TikTok's proposed alternatives to the Act's divestment mandate fail to address the national security concerns, reinforcing the D.C. Circuit's conclusion that the Act is narrowly tailored to address the specific national-security threat. Although TikTok's proposed National Security Agreement would ostensibly insulate TikTok's operations from ByteDance, limit ByteDance's ability to access data, and theoretically give a third party authority over the application of TikTok's algorithm in certain circumstances, *see TikTok*, 2024 WL 4996719, at *4, even prior to the enactment of the Act, the United States government made clear that the proposed agreement does not address the core of its national security concerns. As the D.C. Circuit noted, the proposed NSA would still require substantial trust between the United States and TikTok and ByteDance, *TikTok*, 2024 WL 4996719, at *20. But given ByteDance's refusal to cooperate with government investigations and obfuscation of its operations and data collections practices, it is unsurprising that the United States is unwilling to accept TikTok's eleventh-hour promises that it will insulate operations and limit access by the CCP to sensitive American data. The D.C. Circuit also correctly rejected TikTok's argument that additional reporting and disclosure requirements as well as potential limits on what data the application and its parent company could collect could address the U.S. government's legitimate national security concerns.

These requirements and proposed limitations utterly fail to remedy the harms perpetuated by TikTok's content manipulation or account for the fact that *any* sensitive personal data in the hands of the CCP is a threat to the United States. *Id.* at *22.

The national security concerns addressed by the Act are not just *a* compelling interest for the United States, but perhaps *the most* compelling interest that government might assert on behalf of its citizens. *See Haig v. Agee*, 453 U.S. 280, 307 (1981). Given that the Act goes no further than necessary to address these concerns and to protect the 170 million Americans using TikTok's application—requiring only divestment of foreign ownership at a minimum—the law easily survives even the strictest of scrutiny, as the D.C. Circuit held, *TikTok*, 2024 WL 4996719, at *13, and this Court should affirm.

CONCLUSION

For these reasons, the Court should affirm the decision below.

Respectfully submitted,

THOMAS R. MCCARTHY
KATHLEEN S. LANE
Counsel of Record
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com
katie@consovoymccarthy.com

Counsel for Amici Curiae

December 27, 2024

APPENDIX

APPENDIX TABLE OF CONTENTS

APPENDIX

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 & Nonproliferation, 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

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 Staff Director 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