

Nos. 24-656, 24-657

In the Supreme Court of the United States

TIKTOK INC., ET AL.,

Petitioners,

v.

MERRICK B. GARLAND, ATTORNEY GENERAL,

Respondent.

BRIAN FIREBAUGH, ET AL.,

Petitioners,

v.

MERRICK B. GARLAND, ATTORNEY GENERAL,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT
OF APPEALS FOR THE D.C. CIRCUIT

**BRIEF OF AMERICAN FREE ENTERPRISE
CHAMBER OF COMMERCE AS *AMICUS
CURIAE* IN SUPPORT OF RESPONDENT**

Jonathan Berry
Counsel of Record

Jared M. Kelson

Adam H Chan

Jonathan Feld*

BOYDEN GRAY PLLC

800 Connecticut Ave NW,

Suite 900

Washington, DC 20006

(202) 955-0620

jberry@boydengray.com

William P. Barr

TORRIDON LAW PLLC

801 17th St NW,

Suite 1100

Washington, DC 20006

Counsel for American

Free Enterprise Chamber

of Commerce

*Admitted in Pennsylvania. Limited to
practice in federal courts and agencies.

TABLE OF CONTENTS

INTEREST OF *AMICUS CURIAE*..... 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

 I. SALT TYPHOON UNDERSCORES THE NATIONAL
 SECURITY IMPERATIVE IN PREVENTING PRC
 OWNERSHIP OR CONTROL OF TIKTOK 4

 II. CONGRESS REGULARLY IDENTIFIES SPECIFIC
 ENTITIES IN NATIONAL SECURITY STATUTES 7

 A. *Congress Designates Specific Foreign
 Entities for Sanctions* 8

 B. *Congress Requires the FCC to Effectively
 Ban the Sale of New Products Produced
 by Certain PRC Companies* 11

 C. *Congress Singles Out Specific Entities
 in Other National Security Contexts* 13

 III. THE ACT SURVIVES EVEN STRICT SCRUTINY .. 16

 A. *Compelling Interests Justify the Act* 16

 B. *Prohibiting Foreign Ownership or
 Control Is Narrowly Tailored* 20

CONCLUSION 21

TABLE OF AUTHORITIES

CASES	Page(s)
<i>Aptheker v. Sec’y of State</i> , 378 U.S. 500 (1964)	21
<i>Associated Press v. United States</i> , 326 U.S. 1 (1945)	4, 21
<i>Bank Markazi v. Peterson</i> , 578 U.S. 212 (2016)	15
<i>Bluman v. FEC</i> , 565 U.S. 1104 (2012)	4, 18
<i>Bluman v. FEC</i> , 800 F. Supp. 2d 281 (D.D.C. 2011),	4, 18
<i>Citizen Pub. Co. v. United States</i> , 394 U.S. 131 (1969)	4
<i>Citizens United v. FEC</i> , 558 U.S. 310 (2010)	17
<i>Dep’t of Navy v. Egan</i> , 484 U.S. 518 (1988)	16
<i>Haig v. Agee</i> , 453 U.S. 280 (1981)	16, 21
<i>Hernandez v. Mesa</i> , 589 U.S. 93 (2020)	16
<i>Hikvision USA, Inc. v. FCC</i> , 97 F.4th 938 (D.C. Cir. 2024).....	12

<i>Holder v. Humanitarian L. Project</i> , 561 U.S. 1 (2010)	3, 15, 16
<i>Huawei Techs. USA, Inc. v. United States</i> , 440 F. Supp. 3d 607 (E.D. Tex. 2020)	14
<i>Kaspersky Lab, Inc. v. DHS</i> , 909 F.3d 446 (D.C. Cir. 2018)	14
<i>Moody v. NetChoice, LLC</i> , 603 U.S. 707 (2024)	17
<i>Moving Phones P'ship L.P. v. FCC</i> , 998 F.2d 1051 (D.C. Cir. 1993)	19
<i>Murthy v. Missouri</i> , 603 U.S. 43 (2024)	19
<i>Nat'l Rifle Ass'n v. Vullo</i> , 602 U.S. 175 (2024)	19
<i>Rostker v. Goldberg</i> , 453 U.S. 57 (1981)	15, 21
<i>Williams-Yulee v. Fla. Bar</i> , 575 U.S. 433 (2015)	15
STATUTES	
15 U.S.C. § 1	20
18 U.S.C. § 2334	15
22 U.S.C. § 5202	9, 10
22 U.S.C. § 8514	9

22 U.S.C. § 8772.....	15
22 U.S.C. § 8807.....	8
22 U.S.C. § 8807.....	8, 9
22 U.S.C. § 9404.....	10
22 U.S.C. § 9522.....	10
47 U.S.C. § 1601.....	11, 12
47 U.S.C. § 1601 <i>et seq.</i>	11
47 U.S.C. § 1602(a)	11
50 U.S.C. § 1702.....	8
52 U.S.C. § 30121.....	18
I.R.C. § 501.....	1
Hizballah International Financial Pevention Act of 2015, Pub. L. No. 114-102, 129 Stat. 2205 (2015)	10
Hizballah International Financing Prevention Amendments Act of 2018, Pub. L. No. 115- 272, 132 Stat. 4144 (2018)	10
James M. Inhofe National Defense Authorization Act, Pub. L. No. 117-263, 136 Stat. 2395 (2022)	14
John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018)	12, 14

National Defense Authorization Act of 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017)	13
No TikTok on Government Devices Act, Pub. L. No. 117-328, div. R, 136 Stat. 5258 (2022).....	14
Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024)	2
Protecting Europe's Energy Security Act of 2019, Pub. L. No. 116-92, tit. LXXV, 133 Stat. 2300 (2019), <i>as amended by</i> Pub. L. No. 116-283, 134 Stat. 3388 (2021)	11
Secure and Trusted Communications Networks Act, Pub. L. No. 116-124, 134 Stat. 158 (2019)	11
Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423.....	12
Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, H.R. 5009, 118th Cong. (2024).....	13
Sherman Antitrust Act, Pub. L. No. 51-647, 26 Stat. 209 (1890)	20
OTHER AUTHORITIES	
15 C.F.R. § 791.2.....	7
15 C.F.R. § 791.4.....	7

Dustin Volz, <i>Dozens of Countries Hit in Chinese Telecom Hacking Campaign, Top U.S. Official Says</i> , Wall St. J. (Dec. 4, 2024)	5, 6
Ellen Nakashima, <i>Top Senator Calls Salt Typhoon 'Worst Telecom Hack in Our Nation's History'</i> , Wash. Post (Nov. 21, 2024)	2, 5
John Sakellariadis, <i>Up to 80 Telcos Likely Hit by Sweeping Chinese Hack</i> , PoliticoPro (Nov. 22, 2024).....	6
<i>Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked</i> , Off. of Foreign Assets Control, U.S. Dep't of Treasury (Aug. 13, 2014).....	9
<i>Specially Designated Nationals (SDNs) and the SDN List</i> , Off. of Foreign Assets Control, U.S. Dep't of Treasury (rel. Sept. 10, 2002)	9
Tim Starks, <i>U.S. Government Says Salt Typhoon Is Still in Telecom Networks</i> , Cyber Scoop (Dec. 3, 2024)	6

INTEREST OF *AMICUS CURIAE*¹

American Free Enterprise Chamber of Commerce (“AmFree”) is a nonprofit entity organized consistent with I.R.C. § 501(c)(6). AmFree represents hard-working entrepreneurs and businesses across all sectors of the U.S. economy. Its members are vitally interested in the preservation of free markets, innovation, and the continued viability of our republic.

¹ No party’s counsel authored this brief in whole or in part, and no person or entity other than *amici* or its counsel made a monetary contribution intended to fund its preparation or submission.

SUMMARY OF ARGUMENT

The D.C. Circuit below correctly held that provisions of the Protecting Americans from Foreign Adversary Controlled Applications Act (the “Act”), Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024), applicable specifically to TikTok² do not violate the First Amendment. TikTok.App.24a–57a.³ The court explained that the Act satisfies even strict scrutiny because the federal government has a compelling national-security interest in preventing a foreign adversary from harvesting extensive personal data from more than 170 million Americans and covertly manipulating the content of a major communications platform, and the least restrictive means to address these concerns is prohibiting such foreign ownership or control. *Id.*

Amicus writes to emphasize three points. First, the recent Salt Typhoon hack by the People’s Republic of China (“PRC”) into American telecommunications networks removes any doubt about the need for the Act. In the words of Senator Mark Warner, Chairman of the U.S. Senate Select Committee on Intelligence, Salt Typhoon was the “worst telecom hack in our nation’s history—by far,” which enabled the PRC to gather cellular data on countless Americans, including the President-elect and Vice President-elect. Ellen Nakashima, *Top Senator Calls Salt Typhoon ‘Worst Telecom Hack in Our Nation’s History,’* Wash. Post (Nov. 21, 2024),

² “TikTok” as used in this brief includes the relevant corporate entities ByteDance Ltd. and TikTok, Inc.

³ “TikTok.App.” refers to the appendix to TikTok’s emergency application for an injunction, filed December 16, 2024.

<https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/>. Salt Typhoon confirms the need to prevent PRC ownership or control of one of the largest communications platforms in America.

Second, TikTok insists that being singled out in the Act is particularly strong evidence of a First Amendment violation. *E.g.*, TikTok.Application.21–22. But Congress can make its own determinations on matters of national security, and its decisions are “entitled to deference.” *Holder v. Humanitarian L. Project*, 561 U.S. 1, 33 (2010). Congress regularly names specific entities in legislation designed to protect national security—including media companies controlled by foreign adversaries—and often with far more severe consequences. Doing so is nothing new. Concluding that statutes with specific application to named parties cannot survive the First Amendment would cast doubt on dozens of other statutes designed to protect national security.

Third, compelling interests justify the Act. Preventing the collection of sensitive information by a foreign adversary is plainly a compelling national security interest. TikTok does not dispute whether that interest is compelling, only whether it applies. Pet.App.28–29. This Court has also recognized a compelling interest in preventing illicit manipulation of political discourse by foreign entities. Congress can bar foreign entities from spending in election campaigns—a form of political speech—because “the United States has a compelling interest for purposes of First Amendment analysis in limiting the participation of foreign citizens in activities of American democratic self-government, and in thereby

preventing foreign influence over the U.S. political process.” *Bluman v. FEC*, 800 F. Supp. 2d 281, 288 (D.D.C. 2011) (Kavanaugh, J.), *aff’d*, 565 U.S. 1104 (2012). Stopping the PRC’s covert manipulation of content on one of the largest communications platforms in America prevents similar foreign influence. Indeed, it would be passing strange for the First Amendment to protect for foreign-adversary governments what it expressly forbids Congress and the Executive Branch.

Any remedy must address *both* of these compelling interests. Because Congress determined that ownership or control of TikTok inevitably allows the PRC to access personal data from more than 170 million Americans, prohibiting foreign ownership or control was the *only* option, even if other alternatives were available (they were not) to prevent covert manipulation of content on an American communications platform. This Court has also long recognized in the context of antitrust law that requiring media companies to divest certain holdings can further First Amendment values. *Associated Press v. United States*, 326 U.S. 1, 20 (1945); *Citizen Pub. Co. v. United States*, 394 U.S. 131, 133–35 (1969).

This Court should affirm the judgment below.

ARGUMENT

I. SALT TYPHOON UNDERSCORES THE NATIONAL SECURITY IMPERATIVE IN PREVENTING PRC OWNERSHIP OR CONTROL OF TIKTOK

As the D.C. Circuit outlined below, Congress and the Executive Branch have been keenly aware of the PRC’s years-long campaign to gather extensive data on Americans for intelligence and counterintelligence

purposes. TikTok.App.32a–39a; TikTok.App.83a–85a (Srinivasan, C.J., concurring in part and concurring in the judgment). Both reasonably determined that PRC ownership or control—whether direct or indirect—of certain communications applications, including TikTok, threatened national security because it allows a foreign adversary to capture “large swaths of data” on users that can be used for malign purposes like tracking locations, blackmail, and corporate espionage. TikTok.App.38a–39a.

Recent disclosures about the PRC’s hacking operation into critical American telecommunications infrastructure, known as “Salt Typhoon,” underscores this point. The American public has not received full details on the scope, scale, and threat of Salt Typhoon, but reporting suggests the PRC was successful in gaining access to voluminous personal data on Americans to the detriment of our national security. After receiving classified briefings on Salt Typhoon, Senator Warner described the PRC’s cyber-intrusion as the “worst telecom hack in our nation’s history—by far,” which set his “hair[] on fire.” Nakashima, *supra*. Senator Warner explained that the PRC has compromised “literally thousands and thousands and thousands of pieces of equipment across the country” as part of an “ongoing effort ... to infiltrate telecom systems around the world, to exfiltrate huge amounts of data.” *Id.*

According to Anne Neuberger, U.S. Deputy National Security Advisor for Cyber and Emerging Technology, “[t]he Chinese compromised private companies, exploiting vulnerabilities in their systems as part of a global Chinese campaign that’s affected dozens of countries around the world.” Dustin Volz,

Dozens of Countries Hit in Chinese Telecom Hacking Campaign, Top U.S. Official Says, Wall St. J. (Dec. 4, 2024), <https://www.wsj.com/politics/national-security/dozens-of-countries-hit-in-chinese-telecom-hacking-campaign-top-u-s-official-says-2a3a5cca>. Neuberger continued that the PRC used Salt Typhoon to gain access to at least eight American telecommunications companies and the cellphone data of a “large number of Americans.” *Id.* The Wall Street Journal identified Verizon, AT&T, and T-Mobile as among those compromised, and reported that “President-elect Donald Trump, Vice President-elect JD Vance, senior congressional staffers and an array of U.S. security officials were among scores of individuals to have their calls and texts directly targeted.” *Id.*; *see also* John Sakellariadis, *Up to 80 Telcos Likely Hit by Sweeping Chinese Hack*, PoliticoPro (Nov. 22, 2024), <https://subscriber.politicopro.com/article/2024/11/up-to-80-telcos-likely-hit-by-sweeping-chinese-hack-00191304>.

Salt Typhoon was so sophisticated that American intelligence officials “do not believe any [of the hacked companies] have fully removed the Chinese actors from these networks,” leaving Americans at risk of further intrusions. *Id.* Jeff Greene, the Executive Assistant Director for Cybersecurity for the Cybersecurity and Infrastructure Security Agency, expressed that “it would be impossible for us to predict a time frame on when we’ll have full eviction.” Tim Starks, *U.S. Government Says Salt Typhoon Is Still in Telecom Networks*, Cyber Scoop (Dec. 3, 2024), <https://perma.cc/NHM9-4SE9>.

Salt Typhoon is the latest episode in a pattern of malign PRC cyberactivity to gain access to the

personal data of Americans. *See* TikTok.App.32a–38a. It confirms the threat posed by the PRC, the justification for designating it as a foreign adversary, and the need for the Act. *Cf.* 15 C.F.R. § 791.2 (“Foreign adversary means any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.”); *id.* § 791.4(a)(1) (identifying the PRC as a foreign adversary).

Allowing the PRC to continue exercising ownership or control—whether direct or indirect—over a major communications platform that collects massive amounts of personal data from more than 170 million Americans threatens national security. TikTok.App.38a–41a. The First Amendment does not require that result.

II. CONGRESS REGULARLY IDENTIFIES SPECIFIC ENTITIES IN NATIONAL SECURITY STATUTES

TikTok strenuously objects to being singled out in the Act, arguing this is particularly strong evidence of a First Amendment violation. TikTok.Application.21–22. But Congress regularly identifies specific entities in national security statutes, which impose far more sweeping and severe consequences for those named entities. Holding that Congress may not specify TikTok by statute would not only be incorrect as a matter of common sense and current precedent, but it would also threaten numerous other statutes relevant to national security.

A. *Congress Designates Specific Foreign Entities for Sanctions*

The International Emergency Economic Powers Act (“IEEPA”) gives the President sweeping powers in the event of a national emergency over any transaction in which any foreign person has an interest.⁴ Many sanctions statutes then direct the President to exercise the full extent of those powers to isolate specific entities, effectively cutting them off from the American financial system and prohibiting them from engaging in any transactions in the United States or with American entities. Such statutes are far broader than the Act in this case and do not come with an option for divestment.

Of particular interest, 22 U.S.C. § 8807 requires the President to impose IEEPA sanctions on a foreign adversary-controlled media company. Congress found that “[t]he Islamic Republic of Iran Broadcasting [‘IRIB’] has contributed to the infringement of individuals’ human rights by broadcasting forced televised confession and show trials.” *Id.* § 8807(a)(1). The statute then directed the President to impose sanctions on IRIB and its president, Ezzatollah Zargami. *Id.* § 8807(b)(1). This included placing them “on the list of specially designated nationals and

⁴ 50 U.S.C. § 1702(a)(1)(B) (“[T]he President may ... investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, *any* acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising *any* right, power, or privilege with respect to, or transactions involving, *any* property in which *any* foreign country or a national thereof has *any* interest by *any* person, or with respect to *any* property, subject to the jurisdiction of the United States.” (emphases added)).

blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury.” *Id.* § 8807(b)(1)(B). Persons and entities on this list, and certain of their subsidiaries, are subject to the full range of IEEPA sanctions in which “[t]heir assets are blocked and U.S. persons are generally prohibited from dealing with them.” *Specially Designated Nationals (SDNs) and the SDN List*, Off. of Foreign Assets Control, U.S. Dep’t of Treasury (rel. Sept. 10, 2002), <https://perma.cc/64BT-UUBV>; see *Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked*, Off. of Foreign Assets Control, U.S. Dep’t of Treasury (Aug. 13, 2014), <https://perma.cc/F8NW-E4X5>. The statute does not include a divestment option, although it allows the President to lift sanctions if the Iranian Government undertakes specified actions to respect human rights. 22 U.S.C. § 8514(d).

This statute is hardly unique. Congress has directed sweeping IEEPA sanctions (or similar restrictions) on other named entities for national security reasons. Like the Act, these statutes generally rely on findings of a national security or similar threat, including determinations provided by the Executive Branch. For example—

- In 22 U.S.C. § 5202, Congress made it unlawful to “receive anything of value except informational material from the [Palestine Liberation Organization (‘PLO’)] or any of its constituent groups,” “to expend funds from the PLO or any of its constituent groups,” or “to establish or maintain ... facilities or establishments within the jurisdiction of the

United States at the behest or direction of ... the [PLO].” *Id.* § 5202(a)–(c).

- In 22 U.S.C. § 9404, Congress found that Iran’s Islamic Revolutionary Guard Corps meets the requirements for sanctions under various executive orders and statutes, then directed the President to impose full IEEPA sanctions, with no option for the sanctions to be removed.
- In 22 U.S.C. § 9522, Congress codified sanctions that were previously imposed by executive order against specific, named entities relating to the Russian Federation.
- In the Hizballah International Financial Prevention Act of 2015, Congress required substantial restrictions on financial institutions that aid Hizballah, or entities owned, controlled, or acting on behalf of Hizballah, in violation of existing sanctions. Pub. L. No. 114-102, § 102, 129 Stat. 2205, 2206–07 (2015).
- In the Hizballah International Financing Prevention Amendments Act of 2018, Congress required the President to impose full IEEPA sanctions on “any foreign person that the President determines knowingly provides significant financial, material, or technological support for or to” various Hizballah-related entities. Pub. L. No. 115-272, § 101(a), 132 Stat. 4144, 4145 (2018). Congress then specifically required sanctions against the media companies “al-Manar TV, al Nour Radio, [and] the Lebanese Media Group.” *Id.*

- In the Protecting Europe’s Energy Security Act of 2019, Congress required the President to impose sanctions on any entity that offered assistance for the construction of the Nord Stream 2 pipeline, many of which were plainly known by Congress. Pub. L. No. 116-92, tit. LXXV, § 7503, 133 Stat. 2300, 2300 (2019), *as amended by* Pub. L. No. 116-283, § 1242, 134 Stat. 3388, 3945 (2021).

Congress thus has a well-established history of designating specific entities for sanctions in the context of national security.

B. Congress Requires the FCC to Effectively Ban the Sale of New Products Produced by Certain PRC Companies

Congress has also subjected specific companies to restrictions in national security statutes administered by the Federal Communications Commission (“FCC”). In 2019, Congress passed, and the President signed, the Secure and Trusted Communications Networks Act (“STCNA”), Pub. L. No. 116-124, 134 Stat. 158, *codified at* 47 U.S.C. § 1601 *et seq.* The STCNA requires the FCC to create a list of “covered communications equipment or services” produced by certain entities whose equipment poses “an unacceptable risk to the national security of the United States or the security and safety of United States persons.” 47 U.S.C. § 1601(a), (b)(1). FCC subsidies cannot be used to “purchase, rent, lease, or otherwise obtain” or “maintain” those covered communications equipment or services. *Id.* § 1602(a)(1)(A)–(B).

The STCNA then required, 47 U.S.C. § 1601(c)(3), the FCC to rely on certain determinations when creating and adding to the list, including the “covered telecommunications equipment or services, as defined in” the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018). This statute, discussed below in Part II.C, expressly listed telecommunications equipment or services from five PRC companies—Huawei Technologies Co., ZTE Corp., Hytera Communications Corp., Hangzhou Hikvision Technology Co., and Dahua Technology Co.—and their subsidiaries and affiliates. *Id.* § 889(f)(3), 132 Stat. at 1918. Congress thus singled out five specific companies to be denied federal subsidies based on national security risks, with no option for divestment.

In 2021, Congress passed, and the President signed, the Secure Equipment Act of 2021 (“SEA”), Pub. L. No. 117-55, 135 Stat. 423. The SEA went much further in targeting the same PRC companies than the SCTCNA, directing the FCC to adopt proposed rules and clarify that the FCC “will no longer review or approve any application for equipment authorization” for certain of their telecommunications equipment. *Id.* § 2(a)(1)–(2), 135 Stat. at 423.

In *Hikvision USA, Inc. v. FCC*, 97 F.4th 938 (D.C. Cir. 2024), the D.C. Circuit upheld these restrictions as applied to subsidiaries of Hangzhou Hikvision Technology Co. and Dahua Technology Co. The D.C. Circuit was unconcerned that Congress “took aim at Petitioners” in the two statutes and “clearly expressed its view that Petitioners’ products pose a risk to national security in certain circumstances.” *Id.* at 945.

Congress further singles out specific entities for special consideration in this same context. In the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, for example, Congress identified equipment produced by Shenzhen Da-Jiang Innovations Sciences and Technologies Company Limited (“DJI”) and Autel Robotics, their subsidiaries, affiliates, and partners, and any “[c]ommunications or video surveillance services, including software ... or using equipment” provided by these entities. H.R. 5009, 118th Cong., § 1709(a)(1)(A)–(D) (2024) (signed into law by President Biden Dec. 23, 2024). Congress then required “an appropriate national security agency” to determine whether DJI’s and Autel’s equipment or services threaten national security. *Id.* § 1709(a)(1). The FCC must add them to the list of covered communications equipment or services either upon determination that they threaten national security or if no agency makes a determination within one year. *Id.* § 1709(a)(2), (b).

Imposing limitations on specific entities by statute because of national security concerns is common.

C. Congress Singles Out Specific Entities in Other National Security Contexts

Congress singles out entities in other contexts that implicate national security, too. Congress has repeatedly named specific companies in legislation on government procurement and contracting. For example—

- In the National Defense Authorization Act of 2018, Congress banned certain government use of products developed by the Russian company Kaspersky Lab. Pub. L. No. 115-91, § 1634, 131

Stat. 1283, 1739–40 (2017); *see also Kaspersky Lab, Inc. v. DHS*, 909 F.3d 446 (D.C. Cir. 2018) (upholding this provision against a challenge under the Bill of Attainder Clause).

- In the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Congress prohibited government procurement of certain telecommunications and video surveillance equipment or services from PRC companies Huawei Technologies Co., ZTE Corp., Hytera Communications Corp., Hangzhou Hikvision Digital Technology Co., or Dahua Technology Co. on national security grounds. Pub. L. No. 115-232, § 889(a), (f)(3), 132 Stat. at 1917–18; *see also Huawei Techs. USA, Inc. v. United States*, 440 F. Supp. 3d 607 (E.D. Tex. 2020) (upholding this provision against a challenge under the Bill of Attainder Clause).
- In the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Congress banned procurement from, or contracts with, PRC companies Semiconductor Manufacturing International Corp., ChangXin Memory Technologies, and Yangtze Memory Technologies Corp. for national security reasons. Pub. L. No. 117-263, § 5949, 136 Stat. 2395, 3485–93 (2022).
- In the Consolidated Appropriations Act, 2023, Congress banned TikTok from government devices. No TikTok on Government Devices Act, Pub. L. No. 117-328, div. R, 136 Stat. 5258 (2022).

Congress has also singled out specific entities in terrorism-related litigation. In 22 U.S.C. § 8772, for example, Congress made assets held at the Iranian Bank Markazi available to compensate victims of terrorism in a consolidated enforcement proceeding, identified by docket number. This Court upheld that statute in *Bank Markazi v. Peterson*, 578 U.S. 212, 215 (2016). In 18 U.S.C. § 2334(e)(1), Congress similarly subjected only the PLO and the Palestinian Authority to personal jurisdiction in federal courts, in certain circumstances.

Again, Congress regularly makes legislative determinations about specific entities that raise national security concerns.

* * *

In all these examples, Congress singled out entities for special treatment or consideration, often with consequences far more sweeping than the Act at issue here. Congress did not need to wait for the Executive Branch when making national security determinations, and its decisions are “entitled to deference.” *Humanitarian L. Project*, 561 U.S. at 33; *see also Rostker v. Goldberg*, 453 U.S. 57, 64–65 (1981) (explaining that “perhaps in no other area has the Court accorded Congress greater deference” that “national defense and military affairs”). Moreover, Congress included TikTok in the Act with input from the Executive Branch, which only strengthens that decision. Congress and the Executive Branch “need not address all aspects of a problem in one fell swoop” and “may focus on their most pressing concerns ... even under strict scrutiny.” *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 449 (2015). This is the type of determination that Congress frequently makes.

III. THE ACT SURVIVES EVEN STRICT SCRUTINY

A. *Compelling Interests Justify the Act*

The D.C. Circuit below correctly recognized two compelling interests for the Act: (1) preventing the PRC from harvesting extensive personal data from more than 170 million Americans, and (2) limiting the PRC's ability to covertly manipulate content on American communications platforms, including TikTok. TikTok.App.38a–48a. Preventing the collection of sensitive information by a foreign adversary—which can be used for malign purposes like tracking locations, blackmail, and corporate espionage—is plainly a compelling national security interest for the reasons stated by the D.C. Circuit. TikTok.App.38a–42a. “It is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981) (quoting *Aptheker v. Sec’y of State*, 378 U.S. 500, 509 (1964)). Determinations by Congress (and the Executive Branch) that a foreign adversary’s access to this data constitutes a national security threat are also “entitled to deference.” *Humanitarian L. Project*, 561 U.S. at 33; see also *Hernandez v. Mesa*, 589 U.S. 93, 113 (2020) (“Foreign policy and national security decisions are delicate, complex, and involve large elements of prophecy for which the Judiciary has neither aptitude, facilities, nor responsibility.” (cleaned up)); *Dep’t of Navy v. Egan*, 484 U.S. 518, 530 (1988) (describing the “utmost deference” that “courts have traditionally shown” to foreign policy determinations).

Preventing the PRC from covertly manipulating content on American communications platforms is similarly a compelling interest. In *Moody v.*

NetChoice, LLC, this Court held that the First Amendment generally protects a social media company’s right to moderate content on its platform. 603 U.S. 707, 716–17 (2024). As the Court noted, “[t]o the extent that social-media platforms create expressive products, they receive the First Amendment’s protection,” because “government efforts to alter an edited compilation of third-party expression are subject to judicial review for compliance with the First Amendment.” *Id.*

The Court explained that “it is no job for government to decide what counts as the right balance of private expression—to ‘un-bias’ what it thinks biased, rather than to leave such judgments to speakers and their audiences.” *Id.* at 719. This followed from longstanding precedent on campaign finance law “that the government may not ‘restrict the speech of some elements of our society in order to enhance the relative voice of others.’” *Id.* at 742 (quoting *Buckley v. Valeo*, 424 U.S. 1, 48–49, (1976)); see also *Citizens United v. FEC*, 558 U.S. 310, 354 (2010) (prohibiting government restrictions on corporate political speech “on the ground that it prevents the ‘distorting effects of immense aggregations of wealth’” (quoting *Austin v. Mich. Chamber of Com.*, 494 U.S. 652, 660 (1990))).

But in the same context of campaign finance law, this Court has recognized that the government has a compelling interest in preventing *foreign* entities from manipulating American discourse. In *Bluman*, then-Judge Kavanaugh wrote for a three-judge panel that Congress had a compelling interest in banning foreign

campaign contributions, 800 F. Supp. 2d at 285–86,⁵ a form of political speech. The court reasoned, based on a series of decisions by this Court, that:

It is fundamental to the definition of our national political community that foreign citizens do not have a constitutional right to participate in, and thus may be excluded from, activities of democratic self-government. It follows, therefore, that the United States has a compelling interest for purposes of First Amendment analysis in limiting the participation of foreign citizens in activities of American democratic self-government, and in thereby preventing foreign influence over the U.S. political process.

Id. at 288; *see also id.* at 287 (“The government may exclude foreign citizens from activities ‘intimately related to the process of democratic self-government.’” (quoting *Bernal v. Fainter*, 467 U.S. 216, 220 (1984))). Ultimately, because “spending money to influence voters and finance campaigns is at least as (and probably far more) closely related to democratic self-government than serving as a probation officer or public schoolteacher,” and this Court has upheld the exclusion of foreign citizens from those professions, Congress could prohibit foreign campaign spending. *Id.* at 288–89. This Court affirmed. 565 U.S. 1104.

The concerns in this case are analogous to *Bluman*. The federal government has explained that the PRC

⁵ *See* 52 U.S.C. § 30121(a) (prohibiting foreign nationals from making any campaign donations or independent election expenditures, and barring any person from receiving such donations).

could use TikTok to “interfere with our political discourse” and “manipulat[e] public dialogue.” TikTok.App.30a. As the D.C. Circuit similarly observed, “a foreign government threatens to distort free speech on an important medium of communication. Using its hybrid commercial strategy, the PRC has positioned itself to manipulate public discourse on TikTok in order to serve its own ends.” TikTok.App.43a. In fact, the Act is far more precise than the campaign finance law at issue in *Bluman* because Congress opted not to ban *all* foreign entities from controlling large communications platforms, but only those controlled by foreign adversaries.⁶

TikTok’s contrary interpretation of the First Amendment would yield startling consequences. The federal government “cannot attempt to coerce private parties in order to punish or suppress views that the government disfavors.” *Nat’l Rifle Ass’n v. Vullo*, 602 U.S. 175, 180 (2024); *see also Murthy v. Missouri*, 603 U.S. 43, 77–78 (2024) (Alito, J., dissenting); TikTok.App.43a. It would be passing strange if the First Amendment favored a foreign-adversary government, ensuring it could do precisely what the federal government cannot.

⁶ Concerns about foreign media manipulation have also in part undergirded longstanding FCC restrictions on foreign ownership. *See* TikTok.App.67a–71a (Srinivasan, C.J., concurring in part and concurring in the judgment). In *Moving Phones Partnership L.P. v. FCC*, the D.C. Circuit upheld the FCC’s “ban on alien ownership” of radio licenses under the Communications Act of 1934 “to safeguard the United States from foreign influence in broadcasting,” given “the national security policy” rationale. 998 F.2d 1051, 1055 (D.C. Cir. 1993) (cleaned up).

B. *Prohibiting Foreign Ownership or Control Is Narrowly Tailored*

TikTok erroneously characterizes the Act as a “ban.” *E.g.*, TikTok.Application.3. It is no such thing. The Act prohibits foreign ownership or control of TikTok by a foreign adversary, and imposing a corresponding divestment requirement is not unconstitutional under the First Amendment.

Any remedy must address *both* compelling interests. Because Congress determined that ownership or control inevitably allow the PRC to access personal data from more than 170 million Americans, prohibiting foreign ownership or control was the *only* option, even if other alternatives were available (they were not) to prevent covert manipulation of content on TikTok.

Requiring divestment can also further First Amendment values. In the context of antitrust law, *see, e.g.*, Sherman Antitrust Act, Pub. L. No. 51-647, § 1, 26 Stat. 209 (1890), *codified at* 15 U.S.C. § 1, this Court has long recognized that the federal government can order divestment without violating the First Amendment. In fact, this Court has recognized that requiring divestment can actually *vindicate* First Amendment values:

It would be strange indeed however if the grave concern for freedom of the press which prompted adoption of the First Amendment should be read as a command that the government was without power to protect that freedom.... Surely a command that the government itself shall not impede the free flow of ideas does not afford non-governmental combinations a refuge if they impose restraints

upon that constitutionally guaranteed freedom.... Freedom of the press from governmental interference under the First Amendment does not sanction repression of that freedom by private interests.

Associated Press, 326 U.S. at 20.

Congress can act to stop certain corporate ownership structures without violating—and in fact vindicating—the First Amendment. That is exactly how the D.C. Circuit described the federal government’s interest in preventing the PRC from “distort[ing] free speech on an important medium of communication,” given that “[t]he PRC’s ability to do so is at odds with free speech fundamentals.” TikTok.App.43.

It would be anomalous if the government could order divestment of media companies on antitrust grounds, but not on national security grounds. The First Amendment does not privilege antitrust over national security. *Cf. Rostker*, 453 U.S. at 64–65; *see Haig*, 453 U.S. at 307; *Aptheker*, 378 U.S. at 509. And if the First Amendment “does not sanction [i.e., license] repression of that freedom by private interests,” *Associated Press*, 326 U.S. at 20, then surely it does not sanction repression of that freedom by foreign adversary governments.

CONCLUSION

This Court should affirm the decision below.

Respectfully submitted,

/s/ Jonathan Berry

Jonathan Berry

Counsel of Record

Jared M. Kelson

Adam H Chan

Jonathan Feld*

BOYDEN GRAY PLLC

800 Connecticut Ave NW, *Counsel for American*
Suite 900 *Free Enterprise Chamber*

Washington, DC 20006

(202) 955-0620

jberry@boydengray.com

William P. Barr

TORRIDON LAW PLLC

801 17th St NW,

Suite 1100

Washington, DC 20006

of Commerce

*Admitted in Pennsylvania. Limited to practice in federal courts and agencies.