Nos. 24-656 & 24-657

IN THE

Supreme Court of the United States

TIKTOK, INC., ET AL., PETITIONERS,
v.
MERRICK GARLAND, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES, RESPONDENT.

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

BASED POLITICS, INC., PETITIONER,
v.
MERRICK GARLAND, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES, RESPONDENT.

On Writ of Certiorari to the United States Court of Appeals for the District of Columbia Circuit

BRIEF OF AMICUS CURIAE THE FOUNDATION FOR DEFENSE OF DEMOCRACIES IN SUPPORT OF RESPONDENT

Peter C. Choharis*
Arnon D. Siegel
The Choharis Law Group, PLLC
1300 19th Street, NW, Suite 620
Washington, DC 20036
(202) 422-8312
peter@choharislaw.com
* *Counsel of Record*

LEGAL PRINTERS LLC ● Washington, DC ● 202-747-2400 ● legalprinters.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICUS CURIAE[1]

The Foundation for Defense of Democracies (FDD) is a nonpartisan 501(c)(3) research institute based in Washington, D.C. that focuses on national security and foreign policy. FDD conducts in-depth research, produces accurate and timely analyses, identifies illicit activities, and provides policy options—all with the aim of strengthening the national security of the United States and reducing or eliminating threats posed by adversaries and enemies of the United States and other free nations. FDD does not accept donations from foreign governments. For more information, visit https://www.fdd.org.

BACKGROUND

For decades, the Chinese Communist Party ("CCP" or "Party") has required that the internet, and later web-based companies and their apps, be controlled and then exploited in service of the Party and the interests of the People's Republic of China ("PRC").[2] In September 2004, the CCP passed its

---

[1] Pursuant to Rule 37.6, Amicus Curiae FDD certifies that no party or party's counsel authored this brief in whole or in any part; that no party or party's counsel provided any monetary contribution intended to fund the preparation or submission of this brief; and that no party or person, other than Amicus, or Amicus's counsel, made a monetary contribution intended to fund the preparation or submission of this brief.

[2] Much of this background is based on the report by Rachel Lee, Prudence Luttrell, Matthew Johnson, and John Garnaut, "TikTok, ByteDance, and Their Ties to the Chinese Communist Party, Submission [No. 34] to the [Australian] Senate Select

"Decision on Enhancing the Party's Governance Capability," "which formally designated the internet as a domain for Party control and influence: 'Attach great importance to the influence of new types of media channels, such as the internet, on public opinion. * * * Strengthen the construction of internet propaganda teams and form a strong online positive public opinion.'"[3] In November 2013, the Party introduced the "Decision on 'Some Major Issues Concerning Comprehensively Deepening Reform,'" which declared: "We will straighten out the mechanism for both domestic and overseas propaganda and support key media groups to develop both at home and abroad. We will foster external-facing cultural enterprises and support cultural enterprises to go abroad and expand markets there."[4] In August 2021, the PRC's state news agency, Xinhua, confirmed that TikTok was an integral part of the PRC's domestic and overseas propaganda.[5] Xinhua

---

Committee on Foreign Interference through Social Media" (Mar. 14, 2023) (the "Australian Report"), available at https://www.scribd.com/document/633015202/TikTok-ByteDance-And-Their-Tis-to-the-Chinese-Communist-Party

The Australian Report presents a detailed account of the PRC and its intelligence and military assets' use of social media platforms, especially TikTok and ByteDance, to promote the PRC's (and CCP's) domestic and foreign interests.

[3] *Id.* at 17; *see* John Fitzgerald, "Beijing's Quoqing Versus Australia's Way of Life," INSIDE STORY (Sept. 27, 2016), available at https://insidestory.org.au/beijings-guoqing-versus-australias-way-of-life/.

[4] Xinhua News Agency, "Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform" (Nov. 15, 2013), available at https://archive.ph/hs5gH.

[5] *See* Xinhua News Agency, "Let the Short Video Platform Show

explained that "Various short video apps represented by TikTok have emerged" as "platforms to become 'megaphones' for 'telling the China story well and spreading Chinese voices well.'"[6]

Having identified video apps generally, and TikTok specifically, as means to promote CCP propaganda, the PRC enacted laws and practices that ensured both *de jure* and *de facto* control over these companies to serve the PRC and preserve the CCP's power and influence. Notably, the CCP's extensive control and exploitation of TikTok through its parent ByteDance, and how the CCP exercises this power to pursue China's strategic objectives, both chronicled below, is completely absent from Petitioners' D.C. Circuit Brief ("TikTok's Br.") and Petitioners' Emergency Application for Injunction ("P.I. Appl.") in this Court.

The PRC's Legal Control over ByteDance and TikTok

In 2015, the PRC passed the National Security Law, which "requires citizens and organizations to report acts harming national security and to support national security bodies, public security bodies, and military bodies in their work."[7] China's National Intelligence Law of 2017 obligates all Chinese organizations and citizens to collaborate with state

---

a Good Image of China and Spread a Good Voice of China" (Aug 6, 2021), available at https://archive.ph/qk00A#selection-1499.1-1499.89.

[6] Australian Report, *supra* n.2, at 19 (quoting Xinhua News, *supra* n.5).

[7] China Law Translate, "National Security Law" (July 1, 2015), available at https://www.chinalawtranslate.com/2015nsl/.

intelligence operations.[8] That means that all persons and organizations must "support China's intelligence services by secretly turning over data collected in China or overseas."[9] Also, in 2017, the PRC passed the National Cybersecurity Law, which "compels companies and individuals to make networks, data, and communications available to the police and security services."[10] The Data Security Law of 2021 gives the PRC authority "to access and control private data, including China's 'national' data processed overseas."[11] China's recently revised Counter-Espionage Law of 2023 bolsters the state's authority, making clear that all technological developments, whether designed for civilian or for military use, must be available to state security and intelligence services.[12]

The cumulative effect of these laws is to require companies and their innovations, such as ByteDance and its TikTok app, to serve the Chinese state as much or more than to serve their customers. But the PRC's state authorities do not rely on law alone to

---

[8] China Law Translate, "PRC National Intelligence Law (as amended in 2018)" (June 27, 2017), available at https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

[9] Australian Report, *supra* n.2, at 22 (citation omitted).

[10] Law Info China, "Cybersecurity Law of the People's Republic of China" (Nov. 7, 2016), available at https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3.

[11] China Law Translate, "Data Security Law of the PRC" (June 10, 2021), available at https://www.chinalawtranslate.com/en/datasecuritylaw/.

[12] China Law Translate, "People's Republic of China Counter-Espionage Law (2023 Edition)" (Apr. 26, 2023), available at https://www.chinalawtranslate.com/counter-espionage-law-2023/.

achieve their ends. As it had with many other companies, the PRC assumed control over ByteDance, as well as TikTok and its Chinese sister company, Douyin, by controlling management and infiltrating ByteDance with CCP personnel.

The PRC and CCP's Infiltration of TikTok's Parent, ByteDance

TikTok told Congress that it is almost entirely owned by private parties, including U.S. private equity firms.[13] And it told this Court: "No arm of the Chinese government has an ownership stake—directly or indirectly—in TikTok, Inc. or ByteDance Ltd."[14] Both assertions may be technically true, but both are misleading.

In April 2021, a Cyberspace Administration of China ("CAC")-connected fund, along with two other PRC agencies, acquired a one percent equity stake in Petitioners ByteDance's primary Chinese subsidiary, Beijing ByteDance Technology Co., Ltd. ("Beijing ByteDance," renamed "Douyin").[15] TikTok did not disclose to this Court how this Chinese government fund uses its nominally-small ownership share, called

---

[13] *See* U.S. House Committee on Energy and Commerce, Testimony of Shou Chew, Chief Executive Officer, TikTok Inc., at 6 (Mar. 23, 2023), available at https://d1dth6e84htgma.cloudfront.net/Written_Testimony_of_Shou_Chew_c07504eccf_084e8683f3.pdf?updated_at=2023-03-22T03:10:22.760Z.

[14] P.I. Appl. at 8.

[15] *See* Foundation for Defense of Democracies, "5 Things to know about Bytedance, TikTok's Parent Company" (Mar. 12, 2024) ("FDD Report"), available at https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company; Australian Report, *supra* n.2, at 44. *See generally id.* at 43-48, 32-39; 25-30.

a "golden share," to exercise control over Chinese companies.[16] For example, the one-percent stake jointly held by the CAC-fund and other agencies gives the Chinese government the power to appoint one of Beijing ByteDance three members of the Board of Directors.[17] The Director chosen by CAC was Wu Shugang, Party secretary of the Communist Youth League under the Ministry of Education. Wu gained notoriety in 2012, when he posted, "I only have one wish – that one day I can cut off the dog head of traitors. Let the Chinese traitors preaching so-called 'human rights and freedom' go to hell!!"[18] Wu's authority at Beijing ByteDance includes the "power to control the content at ByteDance's media platforms in China" and "the right to appoint the group's chief censor, known at Chinese internet groups as the 'editor in chief.'"[19]

As a result, the CCP exercises strategic control over ByteDance and its subsidiaries, TikTok and China-focused Douyin. The CCP's control is not focused on commercial matters the way a board member of Western private company would focus—just as it would be extremely rare for a Western company to allow a 1% equity holder to appoint one of only three Board members. Rather, the Party's

---

[16] *See* Ryan McMorrow, Qianer Liu, and Cheng Leng, "China Moves to Take 'Golden Shares' in Alibaba and Tencent Units," FINANCIAL TIMES (Jan. 12, 2023), available at https://archive.md/PmxYE.

[17] *See* FDD Report *supra* n.15, at 12; Australian Report, *supra* n.2, at 44-45.

[18] "The Secretary of the Patriotic Party Said Wildly to Cut Off the Heads of Netizens, and an Office Photo Betrayed Him," APOLLO NEWS (July 17, 2012), available at https://archive.md/yGthO.

[19] *See supra* n.16.

"golden share" allows it to focus on the Party's and Chinese government's strategic goals domestically (in the case of Douyin) and overseas (in the case of TikTok).[20] As set forth in Section I *infra*, these interests include both accessing overseas data about individuals and manipulating content to target individuals or groups of individuals for pro-PRC messaging campaigns.

But while China's legal requirements and its ByteDance board seat have allowed Chinese authorities to gain access to ByteDance's (and TikTok's) strategic objectives, the CCP's greatest power and influence over these companies stem from the Party's practice of infiltrating Chinese technology companies, including ByteDance, with Party members who create "cells" within the companies. "The divide between private and public companies in China has narrowed in recent years through the Party's aggressive expansion of Party organizations within private firms and its use of extra-legal measures to purge prominent leaders within those firms."[21] The removal of Jack Ma, Alibaba's founder, from the company's senior management is perhaps the best known example of this trend; but not surprisingly, the same thing happened to TikTok's Founder and original CEO, Zhang Yiming.[22] But

---

[20] Li Yuan, "China's TikTok Blazes New Ground. That Could Doom It," N.Y. TIMES (Nov. 5, 2019), available at https://web.archive.org/web/20220930033958/https://www.nytimes.com/2019/11/05/business/tiktok-china-bytedance.html.

[21] Australian Report, *supra* n.2, at 32.

[22] As were the Founder-CEOs of Alibaba and Pinduo, ByteDance Founder and CEO Zhang Yiming was also forced to resign in November 2021. *See* Yingzhi Yang and Bhargav Acharya,

Petitioners do not tell this Court any of this and instead dissemble, simply describing Mr. Yiming as a 21% owner of ByteDance Ltd. and "one of its founders" who is a "Chinese national who lives in Singapore." P.I. Appl. at 8.

The CCP "operates party cells throughout ByteDance's hierarchy, affording it direct access to ByteDance's technology and strategic insights" and goals.[23] These "Party structures are not designed to be visible or accountable to international regulators, partners, investors, or consumers"—or U.S. courts—making the extent of its power and influence difficult to estimate or even document.[24] But there is no question that ByteDance exercises enormous control over TikTok irrespective of the legal formalities of the companies' corporate structures.[25] And *Forbes* has reported that "[t]hree hundred current employees at TikTok and ByteDance previously worked for Chinese state media publications," and that fifty of the "employees [] work for or on TikTok, including a content strategy manager who was formerly a Chief Correspondent for Xinhua News," which the U.S. State Department deems "a foreign government

---

"ByteDance Founder Zhang Yiming Steps Down as Chairman," REUTERS (Nov. 3, 2021), available at https://www.reuters.com/article/bytedance-reshuffling-1103-wedn-idCNKBS2HO06L.

[23] FDD Report, *supra* n.15.

[24] Australian Report, *supra* n.2, at 33.

[25] *See id.* at 40-45; *see also supra* n. 22; Juro Osawa, Amir Efrati, and Shai Oster, "TikTok Still Has Key Software Developers in China Despite Effort to Move Offshore," THE INFORMATION (Aug. 26, 2021), available at https://www.theinformation.com/articles/tiktok-still-has-key-software-developers-in-china-despite-effort-to-move-offshore.

functionary."[26] In fact, fifteen ByteDance employees were also employed *at the same time* by Xinhua and other Chinese state media entities, all foreign government functionaries.[27]

Perhaps this explains ByteDance's close connection to China's military and intelligence services. For example, in 2018, ByteDance established the Beijing Academy of Artificial Intelligence at the behest of China's Ministry of Science and Technology.[28] This nominally academic institution uses civilian development of AI technology for military applications, including the promotion of AI in the field of "national defense innovation."[29]

ByteDance's military ties extend to other high-risk defense institutions with links to China's People's Liberation Army. For instance, ByteDance researchers have collaborated on cutting-edge AI research with scientists from the Huazhong University of Science and Technology, which hosts a large number of PRC government-funded and directed defense laboratories working on projects involving, among other things, the development of artificial intelligence and imaging technology for weapons.[30] ByteDance researchers have also worked

---

[26] Emily Baker-White, "LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—And Some Still Do," FORBES (Aug. 11, 2022), available at https://www.forbes.com/sites/emilybaker-white/2022/08/10/bytedance-tiktok-china-state-media-propaganda/.

[27] *Id.*

[28] FDD Report, *supra* n.15.

[29] *Id.*

[30] *See* China Defence Universities Tracker, "Huazhong University of Science and Technology" AUSTRALIAN STRATEGIC POLICY INSTITUTE & INTERNATIONAL CYBER POLICY CENTRE

on developing deepfakes, a type of AI that can spread misinformation and disinformation, with individuals from the People's Public Security University of China, which is involved in developing technological tools for China's repressive public security apparatus, including its Ministry of Public Security.[31]

TikTok/ByteDance's Petition to the D.C. Circuit coyly revealed that "TikTok is not offered in the People's Republic of China,"[32] and instead, its sister company, Douyin, operates in China. But TikTok never explained why. Why would TikTok, an extraordinarily successful Chinese-controlled company with a global reach, not be "offered" in China—especially when there is so much overlap of TikTok and Douyin's leadership and resources?[33] As is typical of ByteDance and its subsidiaries, the reasons for the companies' decisions are not public. But one compelling business need would be to distance TikTok from the PRC's use of Douyin for extensive domestic surveillance and AI technology to monitor and suppress dissent, which would expose TikTok to sanctions by the U.S. and other western

---

(Nov. 18, 2019), available at https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/.

[31] *See* "An Overview of Deepfake: The Sword of Damocles in AI 265," 2020 International Conference on Computer Vision, Image and Deep Learning, CVIDL (July 10, 2020) available at https://archive.ph/VPnsN; *see also* China Defence Universities Tracker, "People's Public Security University of China," AUSTRALIAN STRATEGIC POLICY INSTITUTE & INTERNATIONAL CYBER POLICY CENTRE, available at https://unitracker.aspi.org.au/universities/peoples-public-security-university-of-china/.

[32] TikTok Petition for Review, Doc. # 2053212 (D.C. Cir.), at 16.

[33] *See* Australian Report, *supra* n.2, at 39, 43. *See generally id.* at 39-44.

governments.[34]

In sum, Petitioners wanly describe TikTok, Inc., which provides the TikTok app in the United States, as "an American company" and its "ultimate parent," ByteDance, Ltd., as a "privately held holding company incorporated in the Cayman Islands" that is part of the "ByteDance group," which has other "subsidiaries and controlled affiliates."[35] Later, Petitioners argue that the Government has "expressly disavowed any argument that the courts" should "'pierce the corporate veil' or 'invoke any other relevant exception' to the fundamental principle of corporate separateness." P.I. Appl. at 20 (citation omitted).

The PRC's "golden share" stratagem; its practice of purging of CEO-Founders; its purchase of one percent of the equity of one of the world's largest social media companies through a fund controlled by various state agencies; its appointment of one of only three directors to the Board of a parent despite having only a 1% stake; and its passage of numerous National Security Laws expressly requiring Chinese companies to provide information and subjecting those companies to the will of the Chinese government—none of these has anything to do with corporate structure or veil-piercing. But there is one thing TikTok/ByteDance cannot deny: It has never disclosed any of this to Congress, the D.C. Circuit, or, thus far, to this Court. Petitioners are not "adversary-

---

[34] *See* FDD Report, *supra* n.15; Claire Fu and Daisuke Wakabayashi, "There Is No TikTok in China, but There Is Douyin. Here's What It Is," N.Y. TIMES (Apr. 25, 2024), available at https://www.nytimes.com/2024/04/25/business/china-tiktok-douyin.html.

[35] P.I. Appl. at 8 & n.3.

controlled because Congress said so," P.I. Appl. at 32; they are "adversary-controlled" because the unrebutted facts reveal so.

The remainder of this brief documents what the CCP and Chinese government do and can do with their power over TikTok—and over the American people.

SUMMARY OF ARGUMENT

TikTok, one of the world's most popular social media apps, is a tool of the Chinese Communist Party. The CCP uses TikTok to serve interests of the People's Republic of China—interests contrary to the national security interests of the United States. TikTok and its parent, ByteDance, thus pose serious threats to America. In requiring that ByteDance divest itself of TikTok, Congress has implemented measures to protect America. Those measures are wise, and they are constitutional.

ARGUMENT

I. TIKTOK POSES THREATS TO U.S. NATIONAL SECURITY.

Petitioners TikTok/ByteDance say that this case is about "speech[] content," because the House Committee Report complains about "misinformation, disinformation, and propaganda."[36] But the threat understood by the Congress and the President when passing the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No.

[36] TikTok's Br., Doc. #2060743 (D.C. Cir.) at 50.

118-50, div. H, 138 Stat. 955 (2024) (the "Act"), is far greater than the transmission of information or even disinformation.

> [T]he concern is not just that an app with TikTok's data harvesting and targeted recommendation capabilities could be used as a platform for disseminating propaganda, disinformation, and other messages designed to influence democratic societies. Rather, it is that TikTok has the potential to sway elections, corrode people's faith in democracy, and undermine the will of open societies to compete against China's authoritarian model globally.[37]

In fact, these concerns are not hypothetical, despite what TikTok/ByteDance would have this Court believe.[38] Rather, even the *public* evidence to which the House and Senate had ready access shows that TikTok/ByteDance has already engaged in conduct that has threatened U.S. national security and can do so on a much greater scale should the PRC so decide.

---

[37] Australian Report, *supra* n.2, at 24.
[38] TikTok's Br., Doc. #2060743 (D.C. Cir.), at 50-54.

A. TikTok Has Conducted U.S. Surveillance and Shared Its Results With Beijing.

In December 2022, FBI Director Christopher Wray identified three threats posed by TikTok and ByteDance: "One, it gives them the ability to control the recommendation algorithm, which allows them to manipulate content and if they want to, to use it for influence operations which are a lot more worrisome in the hands of the Chinese Communist Party."[39] Second, TikTok/ByteDance has "the ability to collect data through it on users which can be used for traditional espionage operations."[40] And third, TikTok/ByteDance has "access to the software . . . millions of [users'] devices and that gives them the ability to engage in different kinds of malicious cyber activity."[41] Director Wray made clear that "all of these things are in the hands of a [PRC] government that doesn't share our values and that has a mission that's very much at odds with what's in the best interest of the United States."[42]

Contrary to TikTok's claim that "the Government's own defense of the Act asserts only that China 'could' engage in certain harmful conduct through TikTok, *not that there is any evidence China is currently doing so* or will soon do so," P.I. Appl. at

---

[39] Christopher Wray, "2022 Josh Rosenthal Memorial Talk," GERALD R. FORD SCHOOL OF PUBLIC POLICY, U. MICH. (Dec. 2, 2022), available at https://fordschool.umich.edu/video/2022/christopher-wray-2022-josh-rosenthal-memorial-talk.

[40] *Id.*

[41] *Id.*

[42] *Id.*

2 (italics added), Director Wray's (and Congress's) concerns were not hypothetical. They were based on deep experience and an extensive public (and classified[43]) record that Congress and the Administration well understood when enacting the Act. And as global as TikTok's market dominance may be, China's exploitation of social media must be understood as just a part of the Chinese government's broader strategy to use communications in any future confrontation with its adversaries.[44]

Foreign Interference.

National security analysts have developed the concept of foreign information manipulation and

---

[43] *See* Mark Warner, Chair, U.S. Senate Intelligence Committee, Remarks on Senate Floor (Apr. 23, 2024) ("Many Americans, particularly young Americans, are rightfully skeptical. At the end of the day, they've not seen what Congress has seen. They've not been in the classified briefings that Congress has held, which have delved more deeply into some of the threats posed by foreign control of TikTok."), available at https://www.commerce.senate.gov/2024/4/cantwell-warner-outline-threats-posed-by-foreign-adversaries-weaponization-of-americans-data-technology.

[44] *See* U.S. House Committee on Energy and Commerce, Subcommittee on Communications and Technology, Testimony of Craig Singleton, "Securing Communications Networks from Foreign Adversaries," FOUND. DEF. DEMOC., at 4 (Feb. 15, 2024) ("China's broader communications sector" encompasses hundreds of companies, many of which "have already established themselves as dominant market players in U.S. and allied markets," reflecting "China's deliberate efforts to gain leverage over U.S. decision-making and constrain American actions through the strategic control of vital American communication networks."), available at https://docs.house.gov/meetings/IF/IF16/20240215/116856/HMTG-118-IF16-Wstate-SingletonC-20240215.pdf.

interference ("FIMI") to describe foreign state and non-state actors, and privatized FIMI ("PFIMI") to describe commercial actors, who spread disinformation and manipulate populations. According to a recent Stanford study,[45] by "tapping into a pool of private talent and innovation that has developed in the digital marketing and social media influence industries, the PRC is bolstering its ability to disseminate its narratives and manipulate public discourse on a global scale."[46] The empirical study acknowledged that it had only "a partial glimpse" into the "clandestine" system run by the PRC, yet still was able determine that "covert FIMI in the PRC is an industrial-scale endeavor involving dozens of actors at all levels of society. It involves both national and local governments, the military, the media and the propaganda system, China's intelligence and security services, commercial enterprises, and even organized crime groups."[47]

Director Wray's comments reflect the consensus view of the U.S. intelligence community. This year's Annual Threat Assessment said that "China is demon-strating a higher degree of sophistication in its influence activity, including experimenting with generative AI."[48] "Beijing is

---

[45] Gaute Friis, Nickson Quak, Sara Shah, and Elliot Stewart, "Countering China's Use of Private Firms in Covert Information Operations," STANFORD FREEMAN SPOGLI INST. FOR INT'L STUDIES, at 5 (June 21, 2024), available at https://stacks.stanford.edu/file/druid:fg865kf5598/countering_prc_use_of_private_ firms%20in_IO_gordian_knot_center_ver.pdf.

[46] *Id.*

[47] *Id.* at 7.

[48] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," at 12 (Feb. 5,

intensifying efforts to mold U.S. public discourse," the Assessment continued, "particularly on core sovereignty issues, such as Hong Kong, Taiwan, Tibet, and Xinjiang."[49]

TikTok has announced that it has deployed "expert teams who focus entirely on detecting, investigating, and disrupting covert influence operations"[50] and now "label[s] the accounts and videos of media entities that we know to be subject to editorial control or influence by state institutions."[51] But last-minute reforms—after years of criticism—do not negate the security threat posed by the PRC's use of private firms such as TikTok to spread disinformation, conduct manipulation, and enable interference globally. And they certainly do not undermine Congress's considered judgment that the threats posed by the PRC through TikTok warranted a legislative solution.

Data Collection.

TikTok's data collection is well-documented: "Despite TikTok vowing to curb the practice, it continues to access some of Apple users' most sensitive data, which can include passwords, cryptocurrency wallet addresses, account-reset links,

---

2024), available at https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[49] *Id.*

[50] TikTok, "Covert Influence Operations" (2024), available at https://www.tiktok.com/transparency/en-us/countering-influence-operations/

[51] TikTok, "Labelling State-Affiliated Media Entities" (2024), available at https://www.tiktok.com/transparency/en-us/state-affiliated-media/.

and personal messages."[52] For example, the *Wall Street Journal* has reported that "some employees at TikTok were able to find what they described internally as a list of users who watch gay content on the popular app, a collection of information that sparked worker complaints."[53] "Employees in China also had access to the data," according to former employees, "and at times controlled the permissions for who could view the information."[54] As the Respondent Government's brief in the D.C. Circuit and U.S. media have reported, TikTok also collects data about the views of its American users on topics such as gun control and religion.[55] And in February 2019, ByteDance's subsidiaries Musical.ly and Musical.ly, Inc. entered into a Consent Order and agreed to pay a fine and alter its practices for violating the Children's Online Privacy Protection Act

---

[52] Dan Goodin, "TikTok and 32 Other iOS Apps Still Snoop Your Sensitive Clipboard Data," ARS TECHNICA (June 27, 2020), available at https://arstechnica.com/gadgets /2020/06/tiktok-and-53-other-ios-apps-still-snoop-your-sensitive-clipboard-data/.

[53] Georgia Wells and Byron Tau, "TikTok Tracked Users Who Watched Gay Content, Prompting Employee Complaints," WALL ST. J. (May 5, 2023), available at https://www.wsj.com /articles/tiktok-tracked-users-who-watched-gay-content-prompting-employee-complaints-5966a5f5.

[54] *Id.*

[55] *See, e.g.*, Georgia Wells and Sadie Gurman, "TikTok Collected U.S. Users' Views on Gun Control, Abortion and Religion, U.S. Says," WALL ST. J. (July 27, 2024), available at https://www.wsj.com/tech/tiktok-collected-u-s-users-views-on-gun-control-abortion-and-religion-u-s-says-4fcf19f6?st=hx3cqz2smfrso9s&reflink=article_email_share.

by unlawfully collecting personal data of children.[56] Notwithstanding the promises in the 2019 Consent Order,[57] on August 8, 2024, the FTC brought a civil complaint against TikTok and ByteDance alleging that they violated the privacy rights of children under the same statute and regulations.[58]

Nor is collection of information the only security risk posed by TikTok/ByteDance. The *New York Times* has reported that "TikTok user data [is] shared on" a company platform called "Lark," which "is used every day by thousands of employees of the app's Chinese owner, ByteDance, including by those in China."[59] According to the *Times,* user photos, countries of residence, internet protocol addresses, device and user IDs, and American driver's licenses were all accessible on the Lark platform, "as were

---

[56] *See* Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, *United States v. Music.ly, et al.*, No. 2:19-1439, Doc. # 1-1 (C.D. Cal. Feb. 27, 2019), available at https://www.ftc.gov/system/files/documents/cases/musical.ly_proposed_order_ecf_2-27-19.pdf.

[57] The Stipulated Order addressed violations by Musical.ly, a company bought by ByteDance, of the Children's Online Privacy Protection Act ("COPPA") and its implementing rule (the "COPPA Rule"). *See id.*

[58] *See* Complaint for Permanent Injunction, Civil Penalty Judgment, and other Relief, *United States of America v. ByteDance Ltd., et al.*, No. 2:24-06535, Doc. # 1 (C.D. Cal. Aug. 2, 2024) (alleging violations of COPPA and the COPPA Rule by TikTok, ByteDance, and various affiliates), available at https://www.ftc.gov/system/files/ftc_gov/pdf/bytedance_complaint.pdf.

[59] Sapna Maheshwari and Ryan Mac, "Driver's Licenses, Addresses, Photos: Inside How TikTok Shares User Data," N.Y. TIMES (May 24, 2023), available at https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html.

some users' potentially illegal content, such as child sexual abuse materials. In many cases, the information was available in Lark 'groups'—essentially chat rooms of employees—with thousands of members."[60]

And beyond thousands of ByteDance employees in China viewing sensitive data, "a former employee of ByteDance, TikTok's Beijing-based parent company, has outlined specific claims that the Chinese Communist Party accessed the data of TikTok users on a broad scale, and for political purposes."[61]

TikTok/ByteDance and their affiant simply ignore all of this specific information, with little more than blanket denials. *See, e.g.,* P.I. Appl. at 14-15. These are plainly insufficient to overturn an Act of Congress.

B. TikTok Enables the PRC to Interfere With U.S. Elections, Manipulate Information That Is Sensitive to China, and Conduct Psychological Warfare.

That TikTok enables the PRC to interfere with U.S. elections, manipulate coverage of issues that are sensitive to Beijing, and wage psychological warfare

---

[60] *Id.*

[61] Brian Fung, "Analysis: There is Now Some Public Evidence that China Viewed TikTok Data," CNN BUSINESS (June 8, 2023), available at https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html; see also Alexandra Sternlicht, "Some Ex-TikTok Employees Say the Social Media Service Worked Closely With Its China-based Parent Despite Claims of Independence," FORTUNE (Apr. 15, 2024), available at https://fortune.com/2024/04/15/tiktok-china-data-sharing-bytedance-project-texas/.

has ample empirical support.

Election Interference.

The current Annual Threat Assessment stated point blank: "China is demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI. *TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties* during the U.S. midterm election cycle in 2022."[62] Similarly, in 2022, the National Intelligence Council reported: "Key Judgment: The [Intelligence Community] assesses that China tacitly approved efforts to try to influence a handful of midterm races involving members of both US political parties. * * * We have high confidence in this assessment."[63]

Indeed, the PRC continues to be active in U.S. elections, especially against select down ballot candidates, most recently just this past year. Amicus FDD's Brad Bowman recently testified before Congress that "China * * * attacked both major presidential candidates, in addition to certain congressional candidates who are critical of China."[64]

---

[62] *Supra* n.48 (emphasis added).

[63] National Intelligence Council, "Intelligence Community Assessment, Foreign Threats to the 2022 U.S. Elections," ICA 2022-27259-A, at i (Dec. 23, 2022), available at https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf.

[64] U.S. Committee on House Administration, Testimony of Bradley Bowman and Max Lesser, "American Confidence in Elections: Prohibiting Foreign Interference," FOUND. DEF. DEMOC., at 5 (Dec. 18, 2024), available at https://www.fdd.

Manipulating Information Sensitive to the PRC.

A new "Intelligence Report" by Rutgers University (the "Rutgers Study") declared that "[t]he conclusions of our research are clear: Whether content is promoted or muted on TikTok appears to depend on whether it is aligned or opposed to the interests of the Chinese Government."[65]

More specifically, using the same methods of analysis as did TikTok itself in defense to charges of antisemitism, the Rutgers Study compared relative hashtags used on TikTok and Instagram, TikTok's main competitor in social media.[66] It focused on six issues "directly sensitive" to the PRC: (1) the treatment of China's Uyghurs; (2) the killings in Beijing's Tiananmen Square in 1989; (3) China's annexation and administration of Tibet; (4) Hong Kong; (5) China's claim to Taiwan; (6) and China's claims on the South China Sea. It then added analyses of three additional areas, all relevant to the PRC's geopolitical interests: (1) the Ukraine-Russia war; (2) Kashmir independence; and (3) the Israel-Hamas war. The Study used, as a control group, topics concerning other political issues (not the ones

---

org/wp-content/uploads/2024/12/Bowman-and-Lesser-Testimony-December-18-2024.pdf.

[65] Network Contagion Research Institute (NCRI) and Miller Center on Policing and Community Resilience of Rutgers University, "A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives" (Dec. 2023), available at https://millercenter.rutgers.edu/wp-content/uploads/2024/01/A-Tik-Tok-ing-Timebomb_12.21.23.pdf.

[66] *Id.* at 3.

that were "China-sensitive") and popular culture (such as pop music, video games, and sports). In the control group, hashtags in Instagram compared to TikTok were comparable, well within the ranges expected. For example, the video game Grand Theft Auto 6 was tagged just about evenly, 1:1, as was pop singer Shakira (0.9:1); Taylor Swift was more popular on Instagram (about 2:1) but still within the expected range, since the number of posts with pop culture hashtags on TikTok is approximately half that of Instagram.[67] The same was true for general political topics not specifically a worry of China's: the hashtag "Trump" was 2.2 times more prevalent on Instagram than TikTok, which, adjusted for the observed political biases in the users of the platform, was within the expected range, *id.*; but so was the hashtag "BLM," about 1.9:1. (The hashtag "Biden" was about even, 1:1.) Both were within the expected range given that hashtags related to politics are about twice as common on Instagram as on TikTok.

For China-sensitive topics, however, hashtags were wildly skewed. Hashtags with the word "Uyghur" were eleven times more common on Instagram as on TikTok. *Id.* at 9. "Tibet"-related hashtags were more than 37 times more common on Instagram. *Id.* at 10. "Hong Kong"-related hashtags were 181 times more common on Instagram. For hashtags related to Ukraine, the ratio was 8.5:1; for those supportive of Israel in its fight against Hamas, the ratio was 6.2:1; for those supportive of Kashmiri independence from India, a position considered in China's interests, the ratio was, amazingly, less than one one-thousandth of one percent, Instagram to

[67] *See id.* at 7.

TikTok. It was, as the Study put it, "challenging to imagine that activity of such magnitude could occur on a platform organically, and without the knowledge and consent of the platform itself."[68] The Study concluded: "[W]e assess a strong possibility that content on TikTok is either amplified or suppressed based on its alignment with the interests of the Chinese Government."[69]

Oddly, Petitioners concede that members of the Senate and House raised this very concern and offered many specific examples (P.I. Appl. at 13), but then deny that compelling evidence of PRC content manipulation exists, when they incorrectly assert that "the Government *(wrongly) alleges*" that a recommendation engine for the U.S. TikTok platform "*may reflect foreign influence*." *Id.* at 25 (italics added).

But Petitioners go further than ignoring the *evidence*—not mere allegations—of TikTok's political bias and manipulation. TikTok/ByteDance spends most of its P.I. Application arguing that, whatever the manipulation, the First Amendment protects foreign propaganda, so long as it is done by a (nominal) U.S. entity with a "recommendation engine" located in the United States. *See* P.I. Appl. at 24-27.

On the law, *Meese v. Keene*, 481 U.S. 465 (1987), and *Lamont v. Postmaster General*, 381 U.S. 301 (1965), do not protect the kind of "foreign propaganda" posed by TikTok/ByteDance. P.I. Appl. at 23, 24. Indeed, in *Meese v. Keene* this Court *upheld* a statute affecting "political propaganda" against a First Amendment challenge. 481 U.S. at

---

[68] *Id.* at 15.
[69] *Id.* at 16.

478-85. And *Lamont* involved First Amendment claims by American speakers (*see* 381 U.S. at 305), not a U.S. company (TikTok) controlled by a *foreign* company (ByteDance) that promotes pro-*foreign* content (Chinese) as cultivated by an algorithm controlled by a *foreign* company (ByteDance) that is itself controlled by a *foreign* government (PRC), as is the case here.

In any event, to the extent that *Lamont* and *Meese* might apply, Amicus respectfully submits that this Court should respond to 21st century propaganda and technology with updated, 21st century First Amendment jurisprudence—especially when national security is at stake.

TikTok/ByteDance is also incorrect on the facts. As the D.C. Circuit found, "ByteDance and TikTok Global have taken action in response to PRC demands to censor content *outside* of China." Petitioners' Appendix 36a. Petitioners complain that the lower court should not have relied on classified, *ex parte* evidence to support that finding. *See* P.I. Appl. at 34. But the public record, including from the FBI Director, has made clear that TikTok's recommendation engine is not sequestered in the United States: "the ability to control the recommendation algorithm, which allows them to manipulate content and if they want to, to use it for influence operations which are a lot more worrisome in the hands of the Chinese Communist Party."[70] And as the next subsection on cognitive warfare explains, TikTok's algorithm does far more than peddle propaganda; it is an important tool for the People's

[70] Christopher Wray, "2022 Josh Rosenthal Memorial Talk," *supra* n.39.

Liberation Army to craft weapons with which to wage war.

Cognitive Warfare.

Different authorities use different terms and definitions to describe "psychological warfare," "information warfare," or "cognitive combat." But under any definition, security professionals concur on the basic tenet that the PRC's military and intelligence arms are using personal data, AI, and other technologies to develop psychological and neuro-weapons to undermine cognitively their adversaries.[71]

For example, a 2023 RAND Report found that

> China views psychological warfare, centered on the manipulation of information to influence adversary decisionmaking and behavior, as one of several key components of modern warfare. * * * *The importance placed on psychological warfare is increasingly*

---

[71] *See* Bradley Bowman, ed., "Cognitive Combat: China, Russia, and Iran's Information War Against Americans," FOUND. DEF. DEMOC. at 8-9 & nn. 9-18 (June 2024) ("FDD Monographs"), available at https://www.fdd.org/wp-content/uploads/2024/06/fdd-monograph-cognitive-combat-china-russia-and-irans-information-war-against-americans.pdf. *See also* Annual Threat Assessment, *supra* n.48, at 12 ("**Beijing is expanding its global covert influence posture to better support the CCP's goals**. The PRC aims to sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence. . . . Beijing's growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow's playbook for influence operations.") (bold in original).

> *linked to Chinese military assessments that the cognitive domain will be a key domain of future warfare*.[72]

China security analyst Craig Singleton at Amicus the Foundation for Defense of Democracies describes China's billion-dollars-a-year campaign to build and deploy its cognitive warfare capacities.

> On a basic level, Beijing's discourse strategy seeks to alter global perceptions about Chinese autocracy and Western democracy . . . . In its most extreme form, called "cognitive domain warfare" (认知域作战) by China's People's Liberation Army, the CCP uses discourse power to influence individual and/or group behaviors to favor Beijing's tactical or strategic objectives. This can be achieved by sowing social division, undermining faith in public institutions, introducing conflicting social narratives, and radicalizing groups within a population.[73]

Duke Law School Professor Nita A. Farahany says that the "People's Liberation Army (PLA) is

---

[72] Nathan Beauchamp-Mustafaga, "Chinese Next-Generation Psychological Warfare," RAND at iv-v (June 1, 2023) (emphasis added), available at https://www.rand.org/pubs/research_reports/RRA853-1.html.

[73] Craig Singleton, "China," published in FDD Monographs, *supra* n.71, at 14, available at https://www.fdd.org/wp-content/uploads/2024/06/fdd-monograph-cognitive-combat-china-russia-and-irans-information-war-against-americans.pdf.

investing heavily in cognitive domain operations, including AI research in brain-inspired software, hardware and decision making."[74] An integral part of this process is data collection, AI, and FIMI—enabled by platforms such as TikTok: "Platforms like TikTok exemplify cognitive influence by shaping the beliefs and preferences of its vast user base while collecting data and developing psychogenic profiles of its users. TikTok's algorithm has the power to mold public opinion and exploit user data to shape preferences, biases and beliefs."[75] And while she endorses the Act banning TikTok, Prof. Farahany believes that it is not nearly enough to counter the growing threat posed by the PRC's emerging cognitive warfare capacities:

> While a TikTok ban may take out the first and fattest mole, it fails to contend with the wider shift to cognitive warfare as the sixth domain of military operations under way, which includes China's influence campaigns on TikTok, a mass collection of personal and biometric data from American citizens

---

[74] *See* Nita Farahany, "TikTok is Part of China's Cognitive Warfare Campaign," Opinion, GUARDIAN (Mar. 25, 2023), available at https://www.theguardian.com/commentisfree/2023/mar/25/tiktok-china-cognitive-warfare-us-ban; *see also* Bill Gerts, "Chinese 'Brain Control' Warfare Work Revealed," WASH. TIMES (Dec. 29, 2021) (reporting "three reports by the People's Liberation Army [that] shed light on the depths of China's brain warfare research and [that] show that it has been underway for several years." One PLA report said that the "focus is to attack the enemy's will to resist, not physical destruction,"), available at https://www.washingtontimes.com/news/2021/dec/29/pla-brain-control-warfare-work-revealed/.

[75] Farahany, *supra* n.74.

> and their race to *develop weapons that could one day directly assault or disable human minds*. We ignore this broader context at our peril. (emphasis added).[76]

In sum, TikTok is not merely a tool for Americans to enjoy "propaganda" from the PRC, as TikTok/ByteDance claims.[77] Rather, it is a tool that enables the PLA to obtain data (often covertly) and refine it with AI so that the PLA and the PRC's intelligence services may fashion weapons to conduct psychological warfare against the United States and its allies in times of conflict. The First Amendment does not protect against that. And that is why, as the D.C. Circuit correctly held, "covert manipulation of content is not a type of harm that can be remedied by disclosure." Petitioners' Appendix 54a.

II. DIVESTITURE IS A REASONABLE REMEDY TO ADDRESS THE GRAVE NATIONAL SECURITY THREATS POSED BY TIKTOK AND BYTEDANCE.

As the Government convincingly shows, the Act's divestiture provisions are a reasonable means of addressing the serious threats to national security posed by TikTok and ByteDance.

Deference to the Legislative and Executive Branches.

When assessing the reasonableness of

---

[76] *Id.*

[77] TikTok Br., Doc. # 2060743 (D.C. Cir.), at 50-58.

measures in the national security sphere, the Supreme Court has repeatedly instructed courts to tread lightly. For example, *Holder v. Humanitarian Law Project* involved a challenge to a statute that criminalized providing "material support or resources" to "foreign terrorist organizations."[78] The litigation there, like this case, concerned "sensitive and weighty interests of national security and foreign affairs."[79] Thus, the Court held, the "evaluation of the facts" and "assessment[s]" by both the Executive and the Legislature are "entitled to deference."[80] This is so because judges do not "begin the day with briefings that may describe new and serious threats to our Nation and its people."[81] It is therefore "vital in this context not to substitute . . . [a court's] evaluation of evidence for a reasonable evaluation by the Legislative Branch."[82]

Similarly, in *Trump v. Hawaii*,[83] the Supreme Court upheld against constitutional challenge an executive order touching on core national security issues, and in doing so the Court relied in part on *Humanitarian Law Project* for the proposition that "when it comes to collecting evidence and drawing inferences" on questions of national security, "the lack of competence on the part of the courts is marked."[84] The D.C. Circuit has frequently cited *Humanitarian*

---

[78] 561 U.S. 1, 33 (2010).
[79] *Id.* at 33-34.
[80] *Id.*
[81] *Id.*
[82] *Id.* at 34 (cleaned up; quoting *Boumediene v. Bush*, 553 U.S. 723, 797 (2008), and *Rostker v. Goldberg*, 453 U.S. 57, 68 (1981)).
[83] 585 U.S. 667 (2018).
[84] *Id.* at 704.

Law Project approvingly on this same point.[85]

TikTok/ByteDance Intransigence.

Petitioners complain that they devoted years negotiating with the Government in an attempt to reach an agreed security protocol, but the Government ceased engaging with them "without explaining why." P.I. Appl., at 10. But this account adds nothing to the bottom line: Congress passed the Act after years of fruitless efforts by both the Executive and Legislative branches to reach a viable, amicable solution to stop TikTok/ByteDance's abuses and respond to U.S. national security and privacy concerns. Put another way, after Appellants spent years knowingly failing to address the national security concerns of two Administrations and several Congresses, and after years of failing to end its objectionable practices on its own, TikTok/ByteDance now appears before this Court like some twenty-first century St. Augustine, who famously prayed, "Lord, give me chastity and continence, but not yet!" Appellants ask this Court to substitute its judgment in place of the other two branches to whom national security is entrusted and to approve a deal that the Executive and Legislative branches have rejected. And from an equity point of view, Appellants are asking this Court to use the First Amendment to grant, last-minute absolution for years of Appellants' refusal to alter their conduct to meet U.S. national

[85] *E.g.*, *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256, 267 (D.C. Cir. 2022) (citing in turn *Olivares v. Transportation Sec. Admin.*, 819 F.3d 454, 466 (D.C. Cir. 2016), which quotes *Humanitarian Law Project*); *see also* Gov't Br., Doc. # 2060743 (D.C. Cir.), at 66 (citing *Humanitarian Law Project*).

security interests.

Ample Authority.

Through the Act, Congress and the Executive are simply exercising powers that they have exercised before. For example, TikTok/ByteDance seeks to cloak itself in the First Amendment, but the Communications Act of 1934 generally requires majority American ownership of broadcast licenses (with certain exceptions for minority stakes), 47 U.S.C. § 310(b), and flatly prohibits ownership by a foreign government, *id.* § 310(a)—precisely what the Act does. Appellants argue that this authority is "special" because of bandwidth scarcity (P.I. Appl. at 23), forgetting TikTok's unparalleled market reach, including "more than 170 million monthly American users," which makes TikTok's bandwidth incredibly rare (P.I. Appl. at 6).

And the very real national security concerns posed by TikTok/ByteDance, such as the potential blackmail of American citizens, are hardly novel: Such concerns led the Committee on Foreign Investment in the United States to force a Chinese company to sell the LGBTQ+ dating app Grindr.[86]

The Constitution Is Not a Suicide Pact.

The Background section of this brief

[86] *See, e.g.*, Yuan Yang and James Fontanella-Khan, "Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns," L.A. TIMES (Mar. 6, 2020), available at https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns.

established that TikTok/ByteDance must comply with PRC laws providing extensive access to Chinese-owned companies' data, algorithms, and other information. The CAC can and did appoint one of three Board members to ByteDance, TikTok's parent. And PRC agencies and the CCP have infiltrated ByteDance throughout its management and technical ranks, just as they do with other tech companies.

Part I.A established that TikTok collects or has collected data and personal information about its users, including children and users who view LGBTQ+ related videos. TikTok also shares user data with ByteDance in a chatroom called "Lark," available to thousands of employees. And ByteDance stores user information in the PRC. Part I.B established that TikTok has interfered in the 2022 and 2024 U.S. elections; manipulated information that is sensitive to the PRC and CCP; and has provided data, AI, and other technology that can assist the PLA and PRC intelligence services with their development of a psychological warfare capacity.

TikTok/ByteDance has not mentioned any of these actions or activities—not on its websites, not during Congressional testimony, not in the media, not in its Petition before the D.C. Circuit, and not in its Application to this Court. All of these activities raise national security concerns, and some pose actual threats to U.S. national security. None conceivably is protected by the First Amendment, but they provide a legitimate basis for Congress to take legislative action to address these concerns and dangers.

Finally, even were the First Amendment somehow implicated by Congress's response to these threats, Congress passed the Act in the context of the

PRC's threats to the independence of Taiwan; aggression toward U.S. allies in the South China Sea; challenges to freedom of navigation in contravention of the Law of the Sea Convention; aid to Russia in its war of aggression in Ukraine; spying in the U.S., including trade secrets and spy balloons; and ongoing election interference. The First Amendment surely does not prevent the Congress and the President from responding to undeniable threats. As Justice Robert Jackson famously remarked 75 years ago, the Bill of Rights would become a "suicide pact" unless the courts of our nation "temper * * * doctrinaire logic with a little practical wisdom."[87] This Court should reject TikTok/ByteDance's arguments to the contrary.

[87] *Terminiello v. City of Chicago*, 337 U.S. 1, 37 (dissenting opinion).

CONCLUSION

This Court should affirm the judgment below and uphold the constitutionality of the Act.

Respectfully submitted,

/s/ Peter C. Choharis

Peter C. Choharis*
Arnon D. Siegel
THE CHOHARIS LAW GROUP, PLLC
1300 19th Street, NW, Suite 620
Washington, DC 20036
(202) 587-4478
peter@choharislaw.com

C*ounsel for Amicus Curiae*
Foundation for Defense of Democracies

*Counsel of Record