[redacted]

ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024

Nos. 24-1113, 24-1130, 24-1183

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC. and BYTEDANCE LTD.,

Petitioners,

v.

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

Respondent.

consolidated with

caption continued on inside cover

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

---

PUBLIC REDACTED BRIEF FOR RESPONDENT

TRICIA WELLMAN
Acting General Counsel

JAMES R. POWERS
Chief, Litigation

JENNIFER M. PIKE
Associate General Counsel
Office of the Director of National Intelligence

DIANE KELLEHER
BONNIE E. DEVANY
SIMON G. JEROME
Attorneys, Federal Programs Branch
Civil Division
U.S. Department of Justice

(additional counsel on inside cover)

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

BRIAN D. NETTER
Deputy Assistant Attorney General

MARK R. FREEMAN
SHARON SWINGLE
DANIEL TENNY
CASEN B. ROSS
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys, Appellate Staff
Civil Division, Room 7260
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-3388

[redacted]

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

Petitioners,

v.

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

Respondent.

BASED Politics Inc.

Petitioner,

v.

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

Respondent.

MATTHEW G. OLSEN
Assistant Attorney General for National Security

DEVIN A. DEBACKER
Chief, Foreign Investment Review Section

ERIC S. JOHNSON
Principal Deputy Chief, Foreign Investment Review Section

TYLER J. WOOD
Deputy Chief, Foreign Investment Review Section

EVAN SILLS
Attorney-Advisor, Foreign Investment Review Section
National Security Division
U.S. Department of Justice

BRADLEY BOOKER
General Counsel

KELLY SMITH
Section Chief

NADIN LINTHORST
Assistant General Counsel

TUCKER MCNULTY
Assistant General Counsel

ANN OAKES
Assistant General Counsel
Federal Bureau of Investigation

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), the undersigned counsel certifies as follows:

A. Parties and Amici

Petitioners in these three consolidated cases are TikTok Inc. and ByteDance, Ltd. (No. 24-1113); Brian Firebaugh, Chloe Joy Sexton, Talia Cadet, Timothy Martin, Kiera Spann, Paul Tran, Christopher Townsend, and Steven King (No. 24-1130); and BASED Politics Inc. (No. 24-1183). Merrick B. Garland, in his official capacity as Attorney General of the United States, is the respondent in these cases.

As of this filing, amici properly before the Court are Electronic Frontier Foundation, Freedom of the Press Foundation, TechFreedom, Media Law Resource Center, Center for Democracy and Technology, First Amendment Coalition, Freedom to Read Foundation, Cato Institute, Matthew Steilen, Arizona Asian American Native Hawaiian and Pacific Islander for Equity Coalition, Asian American Federation, Asian Americans Advancing Justice Southern California, Calos Coalition, Hispanic Heritage Foundation, Muslim Public Affairs Council, Native Realities, OCA-Asian Pacific American Advocates of Greater Seattle, OCA-Asian Pacific American Advocates: San Francisco, OCA-Greater Philadelphia, Sadhana, Sikh Coalition, South Asian Legal Defense Fund, Knight First Amendment Institute at Columbia University, Free Press, Pen American

Center, Milton Mueller, Timothy H. Edgar, Susan A. Aaronson, Hans Klein, Hungry Panda US, Inc., Shubhangi Agarwalla, Enrique Armijo, Derek Bambauer, Jane Bambauer, Elettra Bietti, Ashutosh Bhagwat, Stuart N. Brotman, Anupam Chander, Erwin Chemerinsky, James Grimmelmann, Nikolas Guggenberger, G. S. Hans, Robert A. Heverly, Michael Karanicolas, Kate Klonick, Mark Lemley, David S. Levine, Yvette Joy Liebesman, Dylan K. Moses, Sean O'Brien, and Christopher J. Sprigman.

B. Rulings Under Review

These petitions seek review of the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024). There are no prior rulings under review.

C. Related Cases

These cases were not previously before this Court or any other court. Counsel for respondent is not aware of any other case currently pending before this or any other court within the meaning of D.C. Cir. R. 28(a)(1)(C).

/s/ Sean R. Janda
Sean R. Janda

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases: **Page(s)**

Statutes:

Legislative Materials:

Other Authorities:

GLOSSARY

Act	Protecting Americans from Foreign Adversary Controlled Applications Act
CEO	Chief Executive Officer
FBI	Federal Bureau of Investigation
U.S.	United States

INTRODUCTION

For years, Congress and the Executive Branch have maintained serious concerns about the threat to national security posed by TikTok, a social-media platform that is ultimately owned by the Chinese company ByteDance. Those concerns, which are confirmed by the intelligence community, arise primarily from the combination of certain features of TikTok and its ownership by a Chinese company. The Chinese government, which views the United States as a geopolitical rival, has broad authority and practical ability to require Chinese companies to secretly assist China's intelligence, law enforcement, and national-security efforts. Given TikTok's broad reach within the United States, the capacity for China to use TikTok's features to achieve its overarching objective to undermine American interests creates a national-security threat of immense depth and scale.

The concerns are primarily twofold. First, the TikTok application collects vast swaths of sensitive data from its 170 million U.S. users. That collection includes data on users' precise locations, viewing habits, and private messages—and it even includes data on users' phone contacts who do not themselves use TikTok. The United States has long been concerned that the Chinese government could use its robust authority to take control of these data and thus obtain "access to Americans' personal and proprietary information," which China may stockpile

and strategically deploy to undermine the United States' security. 85 Fed. Reg. 48,637, 48,637 (Aug. 11, 2020).

Second, the application employs a proprietary algorithm, based in China, to determine which videos are delivered to users. That algorithm can be manually manipulated, and its location in China would permit the Chinese government to covertly control the algorithm—and thus secretly shape the content that American users receive—for its own malign purposes.

Those grave national-security concerns engendered years of engagement among Congress, the Executive Branch, and ByteDance regarding whether the threats posed by the application could be ameliorated. That engagement involved a long series of unclassified and classified hearings and briefings, as well as negotiations with the company itself. In the end, Congress determined that a legislative solution was warranted and enacted the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024) (Act).

At a high level, the Act requires TikTok to be divested from Chinese ownership. If that control is not severed, other entities (such as mobile application stores) will be forbidden from providing certain services to enable TikTok's continued operation inside the United States. The Act reflects Congress's and the President's considered judgments that nothing short of severing the ties between

TikTok and China could suffice to mitigate the national-security threats posed by the application. The Act also provides authority to the President to require certain other applications controlled by foreign adversaries—defined to include North Korea, China, Russia, and Iran—to be divested from those adversaries.

Petitioners—TikTok and ByteDance, along with various U.S. users of the TikTok application—now challenge the provisions of the Act requiring TikTok's divestment. Petitioners urge that the Act impermissibly burdens First Amendment-protected expressive activities that occur on TikTok. Petitioners dismiss the political branches' determination that those incidental burdens are justified by a compelling national-security interest. In their view, the threat is illusory and unsupported by specific instances of the Chinese government's exploiting TikTok to undermine the United States' national security. But the serious national-security threat posed by TikTok is real, as evidenced by the public record and confirmed by classified information supplied by the intelligence community.

Moreover, China's long-term geopolitical strategy involves developing and pre-positioning assets that it can deploy at opportune moments. The United States is not required to wait until its foreign adversary takes specific detrimental actions before responding to such a threat. As the Supreme Court has repeatedly admonished, "national security decisions are delicate, complex, and involve large elements of prophecy for which the Judiciary has neither aptitude, facilities, nor

responsibility." *Hernández v. Mesa*, 589 U.S. 93, 113 (2020) (alteration and quotations omitted). This Court should reject petitioners' invitation to second-guess the political branches' informed national-security judgments.

In addition to downplaying the national-security risks, petitioners misapply First Amendment law. The statute is aimed at national-security concerns unique to TikTok's connection to a hostile foreign power, not at any suppression of protected speech. TikTok and ByteDance primarily contend that the Act will undercut their ability to engage in expressive activities like content moderation and posting their own content on TikTok. They largely dismiss the divestment option—under which ByteDance's American affiliate could continue engaging in these activities on the platform—as infeasible, in significant part because TikTok's U.S. operations are currently interwoven with operations in China and because China will not permit the export of the proprietary recommendation algorithm. These arguments only underscore the concerns that motivated Congress: TikTok's U.S. operations are ultimately subject to the direction of a Chinese company subject to Chinese laws; those operations require TikTok to share enormous amounts of U.S. users' sensitive data with their Chinese-based counterparts; and China has specifically acted to maintain its ability to exercise control over TikTok.

The Act thus survives any plausibly applicable level of First Amendment scrutiny—including any form of heightened scrutiny. The Act is narrowly tailored

to, and the least restrictive means of, protecting the United States' compelling interest in its national security.

For similar reasons, TikTok's fallback constitutional arguments are mistaken. The statute advances national-security interests while allowing TikTok to continue its operations to the extent consistent with addressing those interests. It is neither a bill of attainder nor a taking.

For their part, the user petitioners focus on the effect that the Act may have on their own expressive activities by potentially forcing the closure of the TikTok platform within the United States. But as those petitioners do not deny, nothing in the Act forbids them from engaging in any expressive activity: even if the Act's prohibitions take effect, they may continue to post and view the same videos on other platforms. Any preference these petitioners may have for using TikTok over those other platforms does not create a constitutional right to TikTok—nor could their preference overcome the national-security interests supporting the Act.

The Court should deny the petitions for review.

STATEMENT OF JURISDICTION

This Court has exclusive jurisdiction to review the Act's constitutionality. Act § 3(a)-(b). Petitioners timely filed petitions for review on May 7 (TikTok), May 14 (Firebaugh), and June 6 (BASED), 2024. Act § 3(c) (allowing challenge up to 165 days after the Act's April 24, 2024, enactment).

STATEMENT OF THE ISSUES

Congress determined that continued ownership of TikTok Inc. by ByteDance, Ltd. poses a national-security risk. The Act thus permits TikTok to continue operating in the United States only if ByteDance executes a "qualified divestiture" of its interest in TikTok.

The questions presented are:

1. Whether the required divestiture violates the First Amendment.

2. Whether the required divestiture is a Bill of Attainder.

3. Whether the required divestiture is a taking.

PERTINENT STATUTES AND REGULATIONS

The Act is reproduced in the addendum to this brief.

STATEMENT OF THE CASE

1. TikTok is a social-media platform through which users may "create, share, and view videos." App.802. The primary feature of TikTok is "the app's For You feed, which opens a collection of videos curated by TikTok's proprietary recommendation engine based on an individual user's interests and how the user interacts with content they watch." App.807. The recommendation algorithm itself is maintained within China, which has forbidden its export. *See* App.156; TikTok Br. 24.

TikTok is operated in the United States by petitioner TikTok Inc., an American company. App.801. TikTok Inc. is owned by TikTok Ltd., which operates the TikTok application globally. Declaration of David Newman, Principal Deputy Assistant Attorney General, National Security Division, Department of Justice ¶12 (Newman Decl.).[1] Both entities are ultimately owned by Beijing ByteDance Technology, "a Chinese internet technology company headquartered in Beijing." App.3. ByteDance originally launched TikTok in the United States in 2017 and later relaunched the platform following ByteDance's acquisition of the video-sharing platform Musical.ly. TikTok Pet. 9 & n.3. Since that time, TikTok has grown into "one of the most popular social media platforms in the world," with "over 170 million users" in the United States. App.3.

2. Since TikTok was launched, the application has generated significant national-security concerns in the political branches. These concerns are primarily grounded in two features of TikTok's operation, combined with TikTok's and ByteDance's "tight interlinkages" with the Chinese government and the Chinese Communist Party. App.3.

[1] This brief uses the term "TikTok" to broadly refer to the worldwide TikTok entities and TikTok application. Where the distinction among the TikTok-named corporate entities is relevant, this brief refers to TikTok Inc. as "TikTok US" and to TikTok Ltd. and the constellation of other entities that own, operate, or otherwise control the TikTok application outside of the United States as "TikTok Global."

First, TikTok collects vast swaths of users' data. The application's "data collection practices extend to age, phone number, precise location, internet address, device used, phone contacts, social network connections, the content of private messages sent through the application, and videos watched." App.3. Chinese law generally requires Chinese companies to "assist or cooperate" with Chinese "intelligence work" and ensures that China and its security agencies have "the power to access and control private data" held by companies. App.4. As a result, the United States has long been concerned that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information," which could allow the Chinese government to, for example, "track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." 85 Fed. Reg. 48,637, 48,637 (Aug. 11, 2020).

Second, TikTok "relies on a proprietary" algorithm based in China that determines the videos sent to users. App.156. That structure gives rise to the prospect that the Chinese government could covertly "control the recommendation algorithm, which could be used for influence operations." App.8 (quotations omitted). In other words, the recommendation algorithm provides an avenue "for the [Chinese government] to influence" the "content on TikTok." App.156. And "[g]iven the sophistication of TikTok's" algorithm, "it would be difficult to detect

malicious changes" to the algorithm implemented by China (or at China's direction). *Id.*

Concerns about TikTok's threat to national security have prompted repeated Executive Branch and congressional action over the past four years. In August 2020, President Trump issued an Executive Order finding that "the spread in the United States of mobile applications developed and owned by companies in [China] continues to threaten the national security, foreign policy, and economy of the United States." 85 Fed. Reg. at 48,637. In particular, the President determined that "TikTok automatically captures vast swaths of information from its users," including "location data and browsing and search histories." *Id.* The President considered that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information," which would allow the Chinese government "to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." *Id.*

Pursuant to pre-existing statutory authority, President Trump directed the Secretary of Commerce to identify transactions related to TikTok that should be prohibited. In September 2020, the Secretary prohibited various commercial transactions related to ByteDance's operations in the United States, based on findings similar to those articulated in the Executive Order. Those prohibitions,

however, never took effect because they were preliminarily enjoined as exceeding the scope of the statutory authority. *See TikTok Inc. v. Trump*, 507 F. Supp. 3d 92 (D.D.C. 2020); *Marland v. Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020); *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73 (D.D.C. 2020). The Executive Order was later rescinded. *See* 86 Fed. Reg. 31,423 (June 11, 2021).

Also in August 2020, President Trump ordered ByteDance to divest all interests and rights in any assets or property used to enable or support ByteDance's operation of TikTok in the United States and any data obtained or derived from U.S. users of TikTok. *See* 85 Fed. Reg. 51,297 (Aug. 19, 2020). That divestment order followed a review of ByteDance's acquisition of Musical.ly by the Committee on Foreign Investment in the United States. The divestment order has not been enforced; the government did not enforce the order while the parties explored whether they could reach a resolution that adequately mitigated the government's national-security concerns. *See* Newman Decl. ¶¶36-48. No such resolution has been reached.

In 2022, Congress directed the Executive Branch to generally require the removal of TikTok from government devices "due to the national security threat posed by the application." App.8-9; *see* No TikTok on Government Devices Act, Pub. L. No. 117-328, div. R, 136 Stat. 5258 (2022). That statute followed the decisions of "several federal agencies, including the Departments of Defense,

State, and Homeland Security," to prohibit "TikTok on devices for which those specific agencies are responsible." App.4. And a "majority of states" have similarly "banned TikTok on state government devices" for similar reasons. *Id.*

3. Against that backdrop, Congress and the Executive Branch continued to assess the national-security threat posed by TikTok and how to mitigate that threat. *See* App.5-12 (timeline of public statements between 2019 and 2024 by Executive Branch officials, legislators, and others). Most recently, Congress conducted a series of classified briefings and hearings conducted in early 2024, including (1) multiple House committee briefings; (2) a House committee hearing; (3) a briefing for the full House; (4) a briefing to Senate staff; and (5) a Senate committee briefing. *See* Newman Decl. ¶122; App.11.

On April 24, 2024, the President signed the Act into law. The Act makes it unlawful for third parties to "distribute, maintain, or update" a foreign adversary controlled application in the United States by providing certain services such as offering the application in a mobile application store. Act § 2(a)(1). There is no dispute in this litigation that the deprivation of these services would practically preclude an application from continuing to be widely offered to American users. To enforce those prohibitions, the Act provides the Attorney General authority to bring suits in district court seeking civil penalties and declaratory and injunctive relief. Act § 2(d).

The Act provides two pathways for designation of an application as a "foreign adversary controlled application." First, the Act itself designates any application "operated, directly or indirectly," by "ByteDance, Ltd."; "TikTok"; or subsidiaries or successors of those companies. Act § 2(g)(3). Second, the Act provides that a "foreign adversary controlled application" also includes any application that (a) is operated by a "covered company" that is "controlled by a foreign adversary" (*i.e.*, that is owned by an entity in North Korea, China, Russia, or Iran, Act § 2(g)(1), (4); 10 U.S.C. § 4872(d)(2)); and (b) is "determined by the President to present a significant threat to the national security of the United States" following an administrative process. Act § 2(g)(3)(B). A "covered company" is in turn defined to generally include a company that operates any application that permits users to interact with each other but to exclude a company that operates an application "whose primary purpose is to allow users to post product reviews, business reviews, or travel information or reviews." Act § 2(g)(2).

The Act's relevant prohibitions take effect 270 days after the designation of an application as a foreign adversary controlled application; for applications owned by ByteDance and TikTok, therefore, the prohibitions take effect 270 days after the Act's enactment—on January 19, 2025. Act § 2(a)(2). At the same time, an application may be removed from the Act's ambit by execution of a "qualified divestiture" that the President determines will result in the application's "no longer

being controlled by a foreign adversary" and that "precludes the establishment or maintenance of any operational relationship between the United States operations" of the application "and any formerly affiliated entities that are controlled by a foreign adversary." Act § 2(c)(1), (g)(6). And the President is permitted to grant a single extension, of no more than 90 days, of the prohibitions' 270-day effective date if the President makes certain certifications regarding the application's progress toward a qualified divestiture. Act § 2(a)(3).

In this way, the Act echoes approaches previously taken by Congress and the Executive Branch to address the national-security risks arising from foreign-owned commercial entities. Congress has long regulated foreign ownership of, or control over, companies operating in particular industries. *See, e.g.*, *Moving Phones P'ship v. FCC*, 998 F.2d 1051, 1055 (D.C. Cir. 1993) (discussing 47 U.S.C. § 310(b)(3)'s restriction on granting radio licenses to foreign-owned corporations); 12 U.S.C. § 72 (nationally chartered banks); 16 U.S.C. § 797 (licenses for dams, reservoirs, and similar projects); 42 U.S.C. §§ 2131-2134 (licenses to use a nuclear facility); 47 U.S.C. § 35 (undersea cable licenses); 49 U.S.C. §§ 40102(a)(15), 41102(a) (air carriers); *cf.* 22 U.S.C. § 611 *et seq.* (requiring certain agents to disclose their relationship to foreign interests). Similarly, the Federal Communications Commission has recently denied or revoked licenses to operate communications lines in the United States in response to increasing "concern[s] about espionage

and other threats from Chinese-owned telecommunications companies." *Pacific Networks Corp. v. FCC*, 77 F.4th 1160, 1162-63 (D.C. Cir. 2023). And Congress has broadly regulated foreign investment in the United States, including authorizing the President to block foreign investment transactions that threaten national security. *See generally* 50 U.S.C. § 4565 (Committee on Foreign Investment in the United States).

Finally, the Act provides for judicial review. Any party seeking to challenge the Act itself or "any action, finding, or determination under" the Act may file a petition for review in this Court, which has "exclusive jurisdiction over any" such challenge. Act § 3.

4. These three consolidated petitions for review of the constitutionality of the Act's provisions relating to TikTok and ByteDance were filed in this Court. One petition, filed by TikTok US and ByteDance, claims that those provisions violate First Amendment speech rights and Fifth Amendment equal protection rights of the companies, constitute an impermissible bill of attainder, and effect an unlawful taking of private property without just compensation. TikTok Pet. 30-65. The other two petitions—collectively filed by eight individuals and a nonprofit organization within the United States that post content on TikTok, *see* Firebaugh Pet. 3-8; BASED Pet. 2—claim that the Act's provisions violate the First Amendment speech rights of U.S. users. Firebaugh Pet. 27-29; BASED Pet. 13-16.

All three petitions seek a declaration that the Act's ByteDance and TikTok provisions are unconstitutional and an injunction prohibiting the Attorney General from enforcing them. TikTok Pet. 65; Firebaugh Pet. 30; BASED Pet. 16.

SUMMARY OF ARGUMENT

Congress passed the Protecting Americans from Foreign Adversary Controlled Applications Act, requiring the Chinese company ByteDance to divest its ownership of TikTok US in light of evidence that the TikTok application's continued operations in the United States pose a risk to national security so long as TikTok is subject to the control of a Chinese company. Under Chinese law, the Chinese government exercises considerable influence and authority over Chinese commercial entities—like TikTok's parent company ByteDance—that can be used to serve that government's ends, which are increasingly counter to U.S. national security. And the Chinese government has exhibited a strategy in many contexts of pre-positioning assets for malign uses to provide maximum leverage in critical situations.

TikTok provides the Chinese government the means to undermine U.S. national security in two principal ways: data collection and covert content manipulation. First, TikTok collects vast amounts of information on its users (and non-users), including sensitive information on millions of Americans. The Chinese government's authority over ByteDance enables it to gain access to and exploit

that information to undermine U.S. national security, including by developing and recruiting intelligence assets, identifying American covert intelligence officers and assets, and blackmailing or coercing Americans. In addition, China's use of artificial intelligence and other tools for analyzing large datasets in ways that are contrary to U.S. national security depend on the sort of bulk data that TikTok collects.

Second, according to the TikTok petitioners (at 6, 24), TikTok's platform is unique primarily by virtue of its proprietary recommendation algorithm that determines which videos users receive (based on data that TikTok collects on those users). That algorithm, which is based in China, is vulnerable to covert manipulation by the Chinese government to mold the content that American users receive. Those covert efforts could be deployed as part of a malign influence campaign against the United States—for example, to promote disinformation or to amplify preexisting social divisions.

The TikTok petitioners' own submissions here confirm that proposals to minimize the Chinese government's influence over the application's American operations—including by potentially entering into a national security agreement with the federal government—would not sufficiently address the national-security risks. ByteDance has never agreed to move the recommendation algorithm for TikTok out of China—and China has prohibited its export in any event—so even

under petitioners' own proposals, U.S. user data would continue to flow to China to train that algorithm. And more generally, any continued entanglement between TikTok and ByteDance would raise national-security concerns, given the porous and open relationship between the Chinese government and Chinese companies: under any such arrangement, the Chinese government would maintain the capability to collect information on Americans and to covertly manipulate the information that Americans receive, all to the detriment of U.S. national security.

The Act does not target activity protected by the First Amendment, as neither collection of data nor manipulation of an algorithm by a foreign power is protected activity. And the Act does not distinguish among speech based on its content, instead focusing on the control of TikTok by a foreign adversary, such that any adverse effects on expression by U.S. persons are indirect and amply justified. The Act thus easily satisfies any plausibly relevant standard of First Amendment scrutiny.

The TikTok petitioners' fallback constitutional arguments lack merit. The Act does not impose the sort of legislative punishment prohibited by the Bill of Attainder Clause because the Act has the nonpunitive purpose of addressing the national-security concerns posed by TikTok and other foreign adversary controlled applications. And even if it did, corporate entities like ByteDance and TikTok cannot invoke the Clause's protections to relieve themselves of complying with

regulatory burdens. And the TikTok petitioners fail to establish that the Act impermissibly deprives them of all economic value, their sole basis for claiming that the legitimate regulation of their business effects a taking.

I. Congress's Divestment Requirement Reasonably Addresses Significant National-Security Threats Occasioned by TikTok's Continued Operation Under Chinese Ownership

After receiving extensive briefings on the intelligence community's assessment of the threat posed by ByteDance and TikTok, Congress enacted the Act at issue here, requiring divestment from Chinese ownership in order for TikTok to continue to operate in the United States. The legislation followed more than a dozen classified and unclassified sessions over the previous three years—including extensive classified briefings from the intelligence community—to consider the threats posed by China in general and TikTok in particular. App.7-12; *see also* H.R. Res. 1051, 118th Cong., 6-9 (2024); App.119-21. These national-security concerns amply justify the Act.

ByteDance and its U.S. affiliate are unique. The TikTok mobile application is used by more than 170 million Americans, providing the company with a wide range of information, including precise location and phone contacts of users. *See* App.3. And its popularity means that many Americans receive news principally through TikTok. *See, e.g.*, App.41 (describing TikTok as the "dominant news platform for Americans under 30"). But TikTok's parent company and

recommendation algorithm are based in China, giving rise to the risk that a foreign adversary will wield TikTok's enormous power to advance its own interests, to the detriment of U.S. national security.

Based on both public and classified information, the "U.S. Intelligence Community assesses that ByteDance and TikTok pose a potential threat to U.S. national security." Declaration of Casey Blackburn, Assistant Director of National Intelligence, Office of the Director of National Intelligence ¶9 (Blackburn Decl.). ByteDance and TikTok represent particularly valuable assets for China to use to advance its own interests at the expense of the United States' interests in "two principal ways." *Id.* First, there is a risk that China "may coerce ByteDance or TikTok to provide the [Chinese government] access to sensitive and personally identifying U.S. user data collected by the TikTok application." *Id.* Second, there is a risk that China "may coerce ByteDance or TikTok to covertly manipulate" its recommendation algorithm to shape the information received by "millions of Americans." *Id.* Worse still, because China's national-security laws would prohibit ByteDance from disclosing such requests, TikTok users could believe that the manipulated content served to them reflected the genuine views of other Americans.

Petitioners contend that Congress was disabled from addressing this potential threat because, in their view, that threat has not materialized. But

Congress can act even if all of the threatened harms have not yet broadly materialized or been detected. The Supreme Court has squarely rejected the proposition that the government must amass "'specific evidence'" that a national-security harm will certainly transpire, holding that the government may properly "confront evolving threats" through "preventive measure[s]." *Holder v. Humanitarian Law Project*, 561 U.S. 1, 34-35 (2010). That principle is especially apposite here, where China has adopted a strategy of pre-positioning assets for malign use at a point of maximum utility for the Chinese government. Moreover, China's malign activities against the United States in related contexts, along with other information collected by the intelligence community and discussed below, demonstrate that the threat is real, not speculative. *See, e.g.*, Blackburn Decl. ¶¶24-35.

A. ByteDance's Ownership of TikTok Raises Distinct National-Security Risks

1. China Seeks to Overtake the United States and Co-Opts Commercial Enterprises to Advance That Geopolitical Objective

The particular risks posed by TikTok arise in the context of intense geopolitical competition between the United States and China. In the context of that competition, China regularly uses nominally private companies to advance its interests.

At a high level, China intends to make itself into "the preeminent power in East Asia and a major power on the world stage." Blackburn Decl. ¶16. As part of its strategy to "surpass the United States in comprehensive national power," China is engaged in a full-spectrum, coordinated effort "to undercut U.S. influence, drive wedges between the United States and its partners," and "foster norms that favor [its] authoritarian system." *Id.*; *see also* Blackburn Decl. ¶¶15, 19. Director of National Intelligence Avril Haines has noted the "extraordinary degree to which China" is developing "frameworks for collecting foreign data" and "us[ing] it to target audiences for information campaigns or other things," as well as pre-positioning capabilities for "future" use "for a variety of means that they're interested in." App.8 & n.43 (quoting Office of the Dir. of Nat'l Intelligence, *Fireside Chat with DNI Haines at the Reagan National Defense Forum* (Dec. 3, 2022), https://perma.cc/3R6F-D4F6/).

In support of its goals, China "aims to sow doubts about U.S. leadership, undermine democracy, and extend [China's] influence abroad," including through "online influence operations." Blackburn Decl. ¶29. These efforts could include attempts to influence U.S. elections and to "magnify U.S. societal divisions." *Id.*

The Chinese government has already engaged in many related malign activities in the United States—including using "economic espionage and cyber theft[] to give its firms a competitive advantage against the United States and its

companies." Blackburn Decl. ¶25. This activity includes "extensive and broad-ranging economic espionage aimed at stealing U.S. technology, commercial information, and trade secrets from many different sectors to benefit the [Chinese government] and Chinese companies." Blackburn Decl. ¶26. The intelligence community reports that "China's hacking program, which spans the globe and thus affects U.S. partners as well, is larger than that of every other major nation, combined." *Id.* China has also been involved in "extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations." Blackburn Decl. ¶31. And China has pursued malign influence operations to further the government's interests, including censorship and transnational repression in the United States to "counter and suppress views [the government] considers critical of [its] narratives, policies, and actions." Blackburn Decl. ¶27, 29; *see also* App.9 & n.52.

"Taiwan, in particular, is a significant potential flashpoint for confrontation between [China] and the United States" because China "claims that the United States is using Taiwan to undermine China's rise." Blackburn Decl. ¶19. In pursuit of its goal of "forced unification with Taiwan," China "will continue to apply military and economic pressure as well as public messaging and influence activities." *Id.*

[redacted]

As part of China's coordinated, whole-of-government strategy to overtake and undermine the United States, China specifically relies on nominally private companies to advance state interests. China blurs the line between government and private enterprise to allow China to exert control over—and require cooperation from—private companies. The Chinese government "tasks leading [Chinese] technology companies 'on a daily basis' with processing bulk data to glean intelligence from them," including "identifying individuals that should be targeted in information manipulation campaigns.'" Global Engagement Ctr., U.S. Dep't of State, *Special Report: How the People's Republic of China Seeks to Reshape the Global Information Environment* 22 (Sept. 28, 2023), https://perma.cc/69VB-HQMH.

[redacted]

Specifically, China has enacted a comprehensive legal regime to ensure that China may access and use data held by Chinese companies for China's own purposes. Under Chinese national-security laws, the Chinese government can require a China-based company to "surrender all its data to the [government], making companies headquartered there an espionage tool of the [Chinese Communist Party]." App.4. As FBI Director Christopher Wray explained to Congress, "the difference between an ostensibly private company and the [Chinese Communist Party] is essentially a distinction without a difference," *Open Hearing: The 2023 Annual Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 118th Cong. 40 (2023) (*Senate 2023 Annual Intelligence Threat Assessment Hearing*), as Chinese laws can be "used as an aggressive weapon" to compel "whatever the Chinese government wants [the company to do] in terms of sharing information or serving as a tool of the Chinese government," *Worldwide Threats to the Homeland: Hearing Before the H. Comm. on Homeland Sec.*, 117th Cong. 75 (2022); *see also generally* Declaration of Kevin Vorndran, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation ¶¶10-13 (Vorndran Decl.); Newman Decl. ¶¶16-25.

China uses this authority to broadly require private corporations to "assist and cooperate with the Chinese government" across a variety of areas. Newman Decl. ¶19; *see also* Vorndran Decl. ¶10. For example, companies are generally

[redacted]

required to "promptly report any clues and provide evidence of any activities endangering national security." Newman Decl. ¶19. Similarly, companies are required to assist Chinese officials in protecting national security and "anti-terrorism work"—both of which are broadly defined. Newman Decl. ¶¶19, 21 (quotations omitted). And Chinese intelligence institutions are generally directed to establish "cooperative relationships with relevant individuals and organizations"—including Chinese companies—to facilitate their "intelligence work both domestically and abroad." Newman Decl. ¶22 (quotations omitted); *see also* App.4 & nn. 11-15 (House Report discussing these laws). Private companies can pose a unique threat to national security because they "enable adversaries to conduct espionage, technology transfer, data collection, and other disruptive activities under the disguise of an otherwise legitimate commercial activity." Vorndran Decl. ¶6.

[redacted]

[redacted]

[redacted]

Finally, China's leveraging of its companies to advance national interests is particularly concerning because it often happens in secret. The Chinese laws governing cooperation with government investigations generally prohibit companies "from revealing when and if the Chinese government has requested any assistance or information from them." Newman Decl. ¶24; *see also* Blackburn Decl. ¶71 (The Chinese National Security Law "prohibits those who comply with the [Chinese government's] requests from disclosing such cooperation publicly."). Thus, companies like ByteDance may be providing China with access to sensitive

[redacted]

personal data or with other assistance in advancing Chinese goals—or undermining American national security—without the awareness of their users or the public.

2. TikTok Is a Uniquely Helpful Asset to China

As discussed, the national-security threat from TikTok arises from two principal sources: (a) data collection and (b) covert content manipulation.

a. *Data collection.* TikTok collects substantial amounts of data from its users. Access by the Chinese government to that data—both individually and in bulk—would pose substantial threats to the United States' national security. That diverse dataset on TikTok users poses a national-security concern because, as Congress recognized, the Chinese government "has shown a willingness to steal Americans['] data on a scale that dwarfs any other [government]." App.8 & n.42 (quoting University of Michigan Ford School, *Christopher Wray: 2022 Josh Rosenthal Memorial talk*, https://perma.cc/S9WA-HJZ6).

TikTok collects vast amounts of personal information, including "age, phone number, precise location, internet address, device used, phone contacts, social network connections, the content of private messages sent through the application, and videos watched." App.3; *see also* App.156 ("TikTok collects tremendous amounts of sensitive data."). This collection includes not only the user's own information, but information about non-users stored in the contact lists in the user's phone. And because the application's algorithm incorporates the user's physical

location, TikTok has access to the precise locations of millions of Americans. Unsurprisingly, that information "can be used for all sorts of intelligence operations or influence operations," App.11 (quoting FBI Director Wray).

TikTok has already demonstrated how U.S. user data may be employed for nefarious purposes. Public reporting suggests that "ByteDance Ltd. employees accessed TikTok user data . . . to monitor the physical locations of specific U.S. citizens." App.8 & n.45 (citing Emily Baker-White, *EXCLUSIVE: TikTok Spied on* Forbes *Journalists*, Forbes (Dec. 22, 2022)). In particular, *Forbes* reported that several ByteDance employees "tracked multiple journalists" and "a small number of people connected to the [journalists] through their TikTok accounts." *Id.*; *see also TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms: Hearing Before the H. Comm. on Energy & Commerce*, 118th Cong. 3, 24, 169 (2023) (describing ByteDance's history of surveilling American journalists); *The Chinese Communist Party's Threat to America: Hearing Before the H. Select Comm. on the Strategic Competition Between the United States and the Chinese Communist Party*, 118th Cong. 24 (2023) (*House Select Committee Hearing on Chinese Communist Party*) (statement of Matt Pottinger, China Program Chairman, Foundation for the Defense of Democracies) (confirming that ByteDance used TikTok "to surveil U.S. journalists

[redacted]

in order to try to identify their sources and to retaliate against their sources"); Newman Decl. ¶98.

Given that risk of surveillance, Senator Warner remarked that "leading news organizations . . . across the world" have since "advis[ed] their investigative journalists not to use TikTok." App.118. Other Members of Congress similarly highlighted these data-collection concerns. *See, e.g.*, App.25 (Rep. Rodgers noting that TikTok "collect[s] nearly every data point imaginable—from people's location, to what they search for on their devices, to who they are connecting with," and "even if someone has never been on TikTok, their personal information is at risk of being collected and abused"); App.109 (Sen. Thune noting that "the Chinese Communist Party is able to gain unlimited access to the account information of TikTok users").

[redacted]

[redacted]

[redacted]

Moreover, former TikTok employees recently reported to the media that TikTok employees "share U.S. user data on [China]-based internal communication systems that China-based ByteDance employees can access" and that "TikTok US also approved sending US data to China several times." Blackburn Decl. ¶89(b); *see also* App.7. Public reporting also indicates that TikTok managers sometimes instruct employees to share users' data with ByteDance without going through official channels. Georgia Wells, *TikTok Struggles to Protect U.S. Data From Its China Parent*, Wall St. J. (Jan. 30, 2024), https://perma.cc/SSD8-J4MB.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

The TikTok petitioners elide the relevant inquiry when they seek to downplay (at 54) the value of the data that could be collected by characterizing it as "aggregate data about the user population's video uploading and consumption behavior." That is not the data about which Congress was concerned. Rather, as noted, TikTok collects personal information about its users and those in their phones' contact lists, as well as real-time information on the physical location of millions of TikTok users. *See* App.3. And some, or all, of that data may be accessible from within China. In 2023, "public reporting revealed that TikTok has stored sensitive financial information, including the Social Security numbers and tax identifications of TikTok influencers and United States small businesses, on servers in China accessible by ByteDance" employees. App.10 & n.58.

[redacted]

The TikTok petitioners do not even attempt to suggest that China would not find those data valuable or that their availability to a foreign adversary—in contrast to the data collected by other technology companies that are not controlled by a foreign adversary—would harm national security. Instead, they rely entirely on their assertion, refuted below, that measures short of the divestment requirement would be sufficient to protect such data. *See infra* pt. I.B. Congress's determination that TikTok, as currently constituted, poses a threat to national security based on its ability to acquire U.S. person data and secretly transfer that data to the Chinese government stands essentially unrefuted.

b. *Covert content manipulation.* China may also covertly manipulate the application's recommendation algorithm to shape the content that the application delivers to American audiences. The backbone of TikTok's appeal is its proprietary content recommendation algorithm, which determines which videos users receive and into which the U.S. government has limited visibility. *See also* Blackburn Decl. ¶¶43-46. By directing ByteDance or TikTok to covertly manipulate that algorithm, China could, for example, further its existing malign influence operations and amplify its efforts to undermine trust in our democracy and exacerbate social divisions. As Senator Warner succinctly put it, TikTok could be "covertly manipulated" by an "authoritarian regime" with a "long track record" of "promot[ing] disinformation." App.118.

Congress reasonably acted to prevent this sort of content manipulation by a hostile foreign power. A foreign power's secret manipulation of the content on social-media platforms to influence the views of Americans for its own purposes poses a grave threat to national security. Among other things, it would allow a foreign government to illicitly interfere with our political system and political discourse, including our elections. The Supreme Court has long recognized that excluding foreign citizens—to say nothing of foreign governments—"from basic governmental processes is not a deficiency in the democratic system but a necessary consequence of the community's process of political self-definition." *Cabell v. Chavez-Salido*, 454 U.S. 432, 439 (1982); *see also, e.g.*, *Ambach v. Norwick*, 441 U.S. 68, 73-74 (1979) ("[S]ome state functions are so bound up with the operation of the State as a governmental entity as to permit the exclusion from those functions of all persons who have not become part of the process of self-government."). Because "[t]he government may exclude foreign citizens from activities 'intimately related to the process of democratic self-government,'" *Bluman v. FEC*, 800 F. Supp. 2d 281, 287 (D.D.C. 2011) (three-judge court) (quoting *Bernal v. Fainter*, 467 U.S. 216, 220 (1984)), *aff'd*, 565 U.S. 1104 (2012), the United States "has a compelling interest" in "limiting the participation of foreign citizens in activities of American democratic self-government," which includes "preventing foreign influence over the U.S. political process," *id.* at 288;

see also Independent Inst. v. FEC, 216 F. Supp. 3d 176, 191 & n.11 (D.D.C. 2016) (three-judge court) (recognizing the "vital importance" of "ensur[ing] that foreign nationals or foreign governments do not seek to influence United States' elections"), *aff'd*, 580 U.S. 1157 (2017). It was reasonable for Congress to be concerned that TikTok would be a powerful platform in the hands of the Chinese government if China were to attempt to manipulate an American election—if, for example, the Chinese government were to determine that the outcome of a particular American election was sufficiently important to Chinese interests.

The threat that ByteDance or TikTok could easily manipulate the algorithm to promote or suppress certain content is not an abstract one. TikTok and ByteDance "employees regularly engage" in a practice called "heating," in which certain videos are manually promoted to "achieve a certain number of video views." App.9 & n.47 (quoting Emily Baker-White, *TikTok's Secret "Heating" Button Can Make Anyone Go Viral*, Forbes (Jan. 20, 2023)). TikTok does not disclose which posts are "heated," and public reporting found that China-based employees had "abused heating privileges," with the potential to dramatically affect how certain content is viewed. One instance "led to an account receiving more than three million views." Baker-White, *TikTok's Secret "Heating" Button*, *supra*; *see also* App.382-83, 390, 392 (noting that TikTok employees can promote certain posts with its "heating" functionality).

Because TikTok has "control over the content received by an enormous daily audience of Americans," the application "could be a powerful tool for manipulating this country's public discourse and public perceptions of events." Blackburn Decl. ¶47. And, as multiple witnesses testified to Congress, China could covertly leverage that tool "to censor or shape the content Americans see." *Id.*; *see also House Select Committee Hearing on Chinese Communist Party*, at 24-25 (statement of Matt Pottinger, China Program Chairman, Foundation for the Defense of Democracies); *Discourse Power: The CCP's Strategy to Shape the Global Information Space: Hearing Before the H. Select Comm. on the Strategic Competition Between the United States and the Chinese Communist Party*, 118th Cong. 55 (2023) (statement of John Garnaut, Senior Fellow, Australian Strategic Policy Institute); App.9 n.53, 11 n.61 (citing this prior testimony).

This sort of manipulation of the algorithm would be difficult to detect, as FBI Director Wray testified in multiple hearings. *See, e.g.*, *Senate 2023 Annual Intelligence Threat Assessment Hearing* 26 (statement of Christopher Wray, Director, FBI) (expressing uncertainty that "we would see" the Chinese government manipulating content on TikTok "if it was happening"); *see also* App.10 (citing FBI Director Wray's testimony). The TikTok petitioners themselves emphasize the importance of the proprietary recommendation engine, highlighting

[redacted]

that the determination of which content should be served (or not served) to users is generally not transparent.

Public reporting indicates that, at least as of 2019, "moderators based in Beijing"—not U.S.-based employees—"had the final call" on approving or blocking certain videos and would "routinely ignore[]" U.S.-based employees' requests "not to block or penalize certain videos" "out of caution about the Chinese government's restrictions and previous penalties on other ByteDance apps." Drew Harwell & Tony Room, *Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses*, Washington Post (Nov. 5, 2019), https://perma.cc/D6KY-NSHG. And even within the United States, a more recent academic study "detected sizable anomalies in the prevalence of both pro- and anti-Chinese Communist Party narratives" on TikTok as compared to a different American social-media platform. Blackburn Decl. ¶64; *see also A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives*, Network Contagion Rsch. Inst. 1 (2023) (finding a "strong possibility that TikTok systematically promotes or demotes content on the basis of whether it is aligned with or opposed to the interests of the Chinese Government"). [redacted]

[redacted]

[redacted]

[redacted]

"Intelligence reporting further demonstrates that ByteDance and TikTok Global have taken action in response to [Chinese government] demands to censor content *outside* of China." Blackburn Decl. ¶54.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

These concerns are only enhanced by TikTok's collection of substantial user data, as discussed. *See supra* pp. 27-35. That data collection may "greatly

[redacted]

[redacted]

enhance[]" China's artificial intelligence capabilities and, in turn, those capabilities may be used more effectively "to augment its influence campaigns, such as amplifying preexisting social divisions, and targeting U.S. audiences." Vorndran Decl. ¶32. Indeed, this is similar to how TikTok uses data collection for commercial purposes: the data collected on individual users is employed to ensure that users receive videos that they are most likely to find compelling.

[redacted]

3. China Would Have Incentive to Capitalize on TikTok in Moments of Extreme Importance

Allowing the Chinese government to remain poised to use TikTok to maximum effectiveness at a moment of extreme importance presents an unacceptable threat to national security. The Chinese government's maintenance of TikTok as a potential threat is of a piece with its general strategy of pre-positioning its assets for use at a time of its choosing.

For example, the intelligence community reports that hackers sponsored by the Chinese government "have pre-positioned for potential cyber-attacks against U.S. critical infrastructure by building out offensive weapons within that infrastructure, poised to attack whenever [China] decides the time is right." Blackburn Decl. ¶26. "The United States has found persistent [Chinese-

[redacted]

[redacted]

government] access in U.S. critical telecommunications, energy, water and other infrastructure. [Chinese government] hackers known as 'Volt Typhoon' hide within [American] networks, lying in wait to use their access to harm U.S. civilians." *Id.*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Perhaps

[redacted]

most significant, ByteDance also owns some of the intellectual property on which TikTok's products and services are based—including, of course, the proprietary algorithm. *See* App.817, 828-29 (TikTok "relies on the support of employees of other ByteDance subsidiaries for some functions, including the development of portions of the computer code that runs the TikTok platform"); App.832-33 (describing how TikTok relies on "custom-made ByteDance software tools"). Taken together, "TikTok US is heavily reliant on" TikTok Global and ByteDance in numerous "operational and technological" ways, which means that China "is well-positioned to maintain some degree of access or influence over" TikTok US. Blackburn Decl. ¶78; *see also* App.817, 828-29, 832-33.

B. Congress Reasonably Determined That the Threat Could Not Be Ameliorated by Narrower Proposals

As discussed above, there should be no room for serious dispute that TikTok as currently constituted poses a potential threat to national security that Congress had a compelling interest in combatting. Petitioners thus focus their energies on alternative measures that, in their view, would adequately mitigate the national-security risk. But Congress and the Executive Branch reasonably concluded that neither the proposed national security agreement that ByteDance and TikTok sought to negotiate with the Executive Branch nor petitioners' other proposed alternatives would suffice.

1. The Proposed National Security Agreement Was Inadequate

The TikTok petitioners largely rely on a proposed national security agreement that was considered and rejected by the Executive Branch. That proposal failed to create sufficient separation between the company's U.S. operations and China, presented materially greater risks than other national security agreements that have been consummated, and failed to adequately address the two major concerns discussed above.

a. At a basic level, the TikTok petitioners' argument that its U.S. operations could be sufficiently insulated from Chinese influence to mitigate the national-security risk without divestment is fundamentally at odds with its insistence that divestment is an infeasible option because of the need for TikTok US to remain integrated with its Chinese partner. Petitioners highlight that the "proprietary recommendation engine" is located in China, and that "[t]he Chinese government has made clear in public statements that it would not permit a forced divestment of the recommendation engine." TikTok Br. 24. They further emphasize that TikTok US could not operate independently from ByteDance, which is located in China, both because ByteDance employees alone have the expertise to operate the algorithm, Br. 22, and because TikTok's commercial success depends on global integration, Br. 23-24. And petitioners stress that "a new owner of TikTok in the United States would at minimum require a data-sharing agreement with

ByteDance" to be commercially viable. Br. 23; *see also* pp. 48-49 *supra* (explaining how TikTok US's operations are intertwined with ByteDance and other ByteDance subsidiaries). Even assuming those representations are true, that required entanglement would only make the potential threat posed by TikTok more concerning.

Congress and the President were not required to accept an arrangement in which TikTok's "algorithm, source code, and development activities" would "remain in China under ByteDance Ltd.'s control and subject to [Chinese] laws"; ByteDance would "continue to have a role" in "TikTok's U.S. operations"; TikTok could "continue to rely on the engineers and back-end support in China to update its algorithms" and "source code"; and TikTok would "continue to send U.S. user data to China." App.4-5. In short, the proposed alternatives, whether agreed to by TikTok or imposed by Congress, would not address either of the significant national-security concerns that arise from TikTok's current operations and structure—to say nothing of the fact that the Executive Branch lacked a "baseline level of trust" that TikTok and ByteDance would sufficiently comply with the proposed agreement. Newman Decl. ¶¶73-115.

TikTok's continued operations in the United States pose risks that are "qualitatively different from those addressed under other national security agreements the Executive Branch has found acceptable." Newman Decl. ¶115. For

one, in other agreements, the Executive Branch has been "able to insist on bright-line, ascertainable steps to isolate the investment at issue from malign foreign influence"—for example, by limiting access to physical facilities or sensitive information. Newman Decl. ¶115(a)(i)-(iii). Similar measures are unavailable in the case of TikTok, because the company maintains that its commercial operations require that data flow to China and that core functions continue to be performed in China. Newman Decl. ¶115(a)(iv). Moreover, the "scope and scale" of the commercial activities that TikTok would have been permitted to continue engaging in under the proposed agreement and the particular features of its platform—including "massive data flows between the United States and [China] and the opacity of TikTok's algorithm"—mean that the Executive Branch would not have "meaningfully be[en] able to guarantee compliance" with the proposal. Newman Decl. ¶115(b)(ii), (c)(i).

Although petitioners place considerable weight on the proposal's so-called "shut-down option," TikTok Br. 16, 27, 59-60; Firebaugh Br. 15, 58, that ostensible authority would not have overcome the difficulties described. The ability to take action in response to noncompliance is effective only if the government could detect noncompliance—but, as explained above, the Executive Branch lacked confidence that it could do so. Regardless, the scope of that proposed authority was substantially more limited than petitioners suggest; the

proposed agreement "allowed for a 'temporary stop' only for a specific list of narrowly scoped" violations and did not provide the government with "discretion to shut down the TikTok platform based on its own independent assessment of national security risk." Newman Decl. ¶114(b)-(c). The Executive Branch thus determined that the shut-down option "was insufficient to mitigate the national security risks," Newman Decl. ¶114(f)—and Congress thus reasonably chose to require divestment rather than the more limited means suggested by TikTok's proposal.

b. The proposal also failed adequately to address the specific risks posed by TikTok's connections to a foreign adversary.

Data collection. The TikTok petitioners emphasize that under their proposal, "protected user data . . . would be stored in the United States in the cloud environment of U.S.-based Oracle Corporation." TikTok Br. 16. But as noted, there is no dispute that under any proposed agreement, TikTok would need to send enormous amounts of data to China to feed the algorithm—indeed, "the company would never agree" to "cease collecting U.S. user data or sending it to Beijing to train the algorithm." Newman Decl. ¶115(a)(iv).

The suggestion that this concern could be mitigated by anonymizing the data is meritless. "Open-source reporting has repeatedly raised concern that supposedly anonymized data is rarely, if ever, truly anonymous." Newman Decl. ¶101. For

[redacted]

example, using ostensibly anonymized data from cell phones, New York Times writers were able to "identify, track, and follow 'military officials with security clearances as they drove home at night'" and "'law enforcement officers as they took their kids to school.'" *Id.*; *see also, e.g.*, *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 343-44 & n.11 (4th Cir. 2021) (explaining how "it is almost always possible to identify people" from otherwise purportedly anonymous locational data); *ACLU v. Clapper*, 785 F.3d 787, 794 n.1 (2d Cir. 2015) ("[I]n the context of most large-scale metadata sets, it would not be difficult to reidentify individuals even if the data were anonymized.").

[redacted]

[redacted]

[redacted]

Content moderation. The TikTok petitioners assert that their proposed "Agreement would guard against foreign manipulation of TikTok's content, including through third-party monitoring of TikTok's content moderation practices, recommendation engine, and other source code." TikTok Br. 16. Given the TikTok petitioners' emphasis on the complexity of TikTok's code, the proprietary nature of the algorithm, and the difficulty that a potential buyer would have in understanding and operating the platform, Congress was entitled to doubt that content manipulation could be adequately monitored by a third party.

In particular, there would be no way to ascertain in real time from the platform's output whether its contents were derived from the ordinary operation of the algorithm or from malign influence. Particular videos might "appear to users

[redacted]

because they are organically popular among Americans, because they are deemed newsworthy by TikTok's content curators," or because China directed the platform's operators "to make those videos appear more frequently." Newman Decl. ¶78(d).

The suggestion that reviewing the source code would be sufficient ignores the size and complexity of the code and the other factors that go into the platform's operation. "Most recently, ByteDance represented to the Executive Branch in 2022 that the Source Code contained 2 billion lines of code," which Oracle estimated would take "three years to review." Newman Decl. ¶80. By comparison, the "Windows Operating System contains approximately 50 million" lines of code. *Id.* The United States does not have the capacity to accomplish the herculean task of analyzing and monitoring billions of lines of code. *See* Vorndran Decl. ¶46 (The FBI "does not have agents or analysts devoted to monitoring [national security agreements]."); Newman Decl. ¶79 ("Because of the size and technical complexity of the TikTok platform and its underlying software," ensuring compliance "would require resources far beyond what the U.S. government and Oracle possess.").

Moreover, "[e]ven assuming every line of Source Code could be monitored and verified," China "could exert malign influence through the very same features that have made the TikTok platform globally successful." Newman Decl. ¶78(b). The "heating" feature described above, *supra* p. 37, may "be used to drive views of

[redacted]

content of [China's] choosing." *Id.* Reviewing source code would not ensure that such "features would be used for benign commercial ends, not malicious ones, thus inhibiting the government from detecting noncompliance." *Id.*

[redacted]

2. Petitioners' Alternative Proposals Would Not Adequately Address the National-Security Risks

Petitioners' other alternative proposals fare no better. Petitioners' suggestions that Congress could have required TikTok to disclose its content-moderation policies and permit independent researchers to examine content fail to account for Congress's data-security concerns. And even as to content-moderation, Congress's fundamental concern is that the Chinese government could *covertly* manipulate content on the application. That covert manipulation would not, of course, be disclosed in TikTok's policies. Similarly, the notion that the government

[redacted]

could "simply engage in speech of its own to counter any alleged foreign propaganda," Firebaugh Br. 54, ignores Congress's concern for covert foreign-adversary manipulation that could not be detected.

Finally, the TikTok petitioners' argument (at 59) that Congress "could have extended the ban on the use of TikTok on government devices to federal employees' and contractors' personal devices" fails to meaningfully grapple with the national-security threat posed by TikTok. For one, TikTok may be used to gather data on users and non-users alike, as explained. *See supra* pp. 27, 31-32. That potential threat cannot be ameliorated by a narrower restriction on use of the application by certain groups. Regardless, many of the specific data-security concerns discussed above go far beyond concerns related to China's collection of data regarding current federal employees and contractors. Instead, those concerns extend both to China's bulk collection of data and to China's targeted collection on individuals who are not federal employees—including, for example, family members or potential future government employees (many of whom may be teenagers today, a particular problem given TikTok's popularity among young people). And in any event, Congress is fully entitled to legislate in the interest of all Americans' data security; it is not required to limit itself to protecting the security of federal employees and contractors.

II. The Act Satisfies Any Plausibly Relevant First Amendment Standard

A. The Act Addresses National-Security Concerns and Does Not Target Protected Expression

As explained, *see supra* Part I, the Act addresses the threats posed by China's potential control of TikTok—and, in particular, the national-security harms that accompany China's ability to exploit TikTok to access Americans' sensitive personal information and to covertly manipulate the information that Americans consume. Those harms that the Act aims to ameliorate do not themselves arise from protected First Amendment activity. Obviously, the collection of Americans' data is not itself expressive activity. And China (a foreign state), as well as ByteDance and TikTok Global ("foreign organizations operating abroad"), have "no First Amendment rights," much less a First Amendment right to covertly manipulate the information reaching Americans. *Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l, Inc.*, 591 U.S. 430, 436 (2020).

That holds equally true for TikTok US, ByteDance's and TikTok Global's wholly owned and controlled corporate subsidiary in the United States that runs on technology developed and maintained in China. *Cf. Viereck v. United States*, 318 U.S. 236, 244 (1943) (describing registration and disclosure requirements for those acting as publicity, propaganda, or public-relations agents for foreign principals); *Meese v. Keene*, 481 U.S. 465, 469 (1987) (same). Although the curation of content on TikTok by the Chinese-controlled "proprietary recommendation

engine," TikTok Br. 6, is itself a form of speech, that speech does not enjoy any First Amendment protection because it is—by the TikTok petitioners' own admission, *see* TikTok Br. 24—the speech of a foreigner.

Petitioners thus focus on the Act's incidental effects on expressive activity, such as the speech of American content creators on TikTok or activity in which TikTok US may itself engage (for example, content moderation independent of the recommendation algorithm or posting on the platform). But that activity is not the Act's target. To the contrary, Congress expressly authorized the continuation of those expressive activities on TikTok so long as the national-security harms could be mitigated by eliminating, through divestment, the opportunity for the Chinese government to use TikTok to collect Americans' data or covertly manipulate the information they receive. And TikTok users in the U.S. have the option of turning to other platforms.

The TikTok petitioners' contention that divestment is not legally or practically feasible does not advance their arguments. TikTok Br. 24, 31; App.156. For one, Congress's inclusion of the divestment option underscores the nature of Congress's true concerns—the control of TikTok, not the content on the platform—whether or not ByteDance believes it can ultimately divest. Regardless, if petitioners are correct that the content-recommendation algorithm cannot be exported outside of China and that the remaining aspects of the application

(divorced from the algorithm) are not valuable or popular, that conclusion only highlights the fundamental national-security concerns underlying the statute. *See supra* Part I. On the other hand, if TikTok's operations in the United States have value separate and apart from the algorithm—such as through the application's user base and brand value—it is hard to imagine that TikTok or ByteDance would choose to abandon that substantial value by refusing to divest. And in that scenario, the incidental burdens that the Act places on users' speech would be further minimized.

At most, then, the statute has an incidental effect on protected activity in the United States. As the Supreme Court explained in *United States v. O'Brien*, 391 U.S. 367, 377 (1968), such statutes are permissible so long as they further a substantial governmental interest unrelated to the suppression of free expression and "the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." The national-security interests set forth above are not just substantial, but compelling, and divestment is narrowly tailored to address those interests. And the statute here has even less of an effect on protected activity than the statute at issue in *O'Brien*, which prohibited the burning of draft cards and thus precluded an entire form of protest. Here, the Act prohibits an ownership structure that gives a foreign adversary control over TikTok, but it does not prohibit any category of protected speech, even incidentally. The user

petitioners, for example, have no First Amendment right to TikTok, the algorithm it uses, or a platform subject to Chinese control.

In that respect, the Act is more like the enforcement action upheld in *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706-07 (1986), when the government sought to close a bookstore because it presented a public-health nuisance. Even though a bookstore indisputably facilitates First Amendment activity, bookstores may not "claim special protection from governmental regulations of general applicability simply by virtue of their First Amendment protected activities." *Id.* at 705. And the lack of any First Amendment violation was underscored because the relevant parties "remain[ed] free to" engage in the same expressive activity "at another location." *Id.* Similarly, in *Virginia v. Hicks*, 539 U.S. 113 (2003), the Supreme Court upheld a statute that forbade the reentry of any person with prior civil violations into an otherwise open public forum. As the Court explained, even as applied to persons who wish to engage in expressive activity in the forum, enforcement of the statute "no more implicate[d] the First Amendment than would the punishment of a person who has (pursuant to lawful regulation) been banned from a public park after vandalizing it, and who ignores the ban in order to take part in a political demonstration." *Id.* at 123.

In short, the alleged burdens on petitioners' speech are purely incidental, and "the First Amendment does not prevent restrictions directed at commerce or

conduct"—like those here—"from imposing incidental burdens on speech." *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 567 (2011). And even that incidental burden leaves open multiple alternative channels for communication. The challenged provisions of the Act restrict the ownership of a single social-media application, leaving open numerous other well-known platforms, including several that provide venues for short-form videos similar to those posted on TikTok—such as Facebook, Instagram, Snapchat, Twitter (now "X"), and YouTube, among others. *See Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2395 (2024) ("The biggest social-media companies—entities like Facebook and YouTube—host a staggering amount of content."); *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 479-80 (2023) (describing how Facebook, YouTube, and Twitter are "three of the largest and most ubiquitous platforms on the internet" and "[o]n YouTube alone, users collectively watch more than 1 billion hours of video *every day*").

Despite the availability of alternative platforms, the user petitioners seek to convert their preference for using TikTok into a First Amendment right to the platform's continued existence. But it is well established "that the First Amendment does not guarantee the right to communicate one's views at all times and places or in any manner that may be desired." *Heffron v. International Soc'y for Krishna Consciousness, Inc.*, 452 U.S. 640, 647 (1981). Even in the context of time, place, and manner regulations, which—unlike the Act—directly regulate

speech in the United States, the government may permissibly impose restrictions that "reduce to some degree the potential audience for . . . speech." *Ward v. Rock Against Racism*, 491 U.S. 781, 802 (1989). In *Kovacs v. Cooper*, 336 U.S. 77 (1949), for example, the Supreme Court upheld an outright prohibition on a means of expression—namely, sound trucks. "That more people may be more easily and cheaply reached by sound trucks" is "not enough to call forth constitutional protection for what those charged with public welfare reasonably think is a nuisance when easy means of publicity are open." *Id.* at 88-89. The Firebaugh petitioners' argument (at 59-60) that the government's national-security interests must be disregarded merely because TikTok is their "primary method of engaging with audiences they cannot reconstitute elsewhere" cannot be reconciled with this precedent.

The Firebaugh petitioners' reliance (at 27-28) on *City of Ladue v. Gilleo*, 512 U.S. 43 (1994), is misguided. There, the Supreme Court analyzed an ordinance prohibiting the display of nearly all signs on homeowners' property as a time, place, and manner regulation that failed to leave open alternative channels because it "almost completely foreclosed a venerable means of communication that is both unique and important." *Id.* at 54-56. The First Amendment concerns occasioned by a direct restriction on a form of expression that "carrie[d] a message quite distinct from" the alternatives identified, *id.* at 56, are different in kind from petitioners'

objection that the Act could cause them to choose other platforms that they consider inferior in certain respects but that nonetheless offer broad opportunities to post video content on the internet, *see* Firebaugh Br. 28-30. In other words, although petitioners express a preference for using TikTok, nothing about the Act materially inhibits their "ability to communicate effectively" on the wide variety of other available platforms. *Members of the City Council of L.A. v. Taxpayers for Vincent*, 466 U.S. 789, 812 (1984).

B. Petitioners' Arguments for Heightened Scrutiny Fail

Although the Act directly regulates conduct unprotected by the First Amendment (a foreign adversary's control of a company that raises significant national-security risks), petitioners nonetheless contend that the Act's restrictions on TikTok are subject to heightened scrutiny. That is so, according to petitioners, because the Act draws content- and speaker-based distinctions, because it singles out TikTok, and because it burdens users' associational rights.

As discussed below, none of those justifications for heightened scrutiny applies here. But in any event, even if heightened scrutiny were to apply, it would clearly be satisfied in light of the national-security interests at stake. *See supra* Part I. This Court has repeatedly recognized that "[i]n the national security context, 'conclusions must often be based on informed judgment rather than concrete evidence, and that reality affects what we may reasonably insist on from the

Government.'" *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256, 266 (D.C. Cir. 2022) (quotation omitted). The Supreme Court has similarly cautioned against judges' attempts to second-guess the political branches' necessarily predictive judgments on matters of national security. *See Humanitarian Law Project*, 561 U.S. at 34-35 (recognizing that when taking "preventive measure[s]" to "confront evolving threats" in the national-security context, the political branches may permissibly rely "on informed judgment rather than concrete evidence").

Indeed, petitioners err in focusing on the lack of congressional findings in the Act, going so far as to claim that "the absence of statutory findings by itself requires the Act's invalidation." TikTok Br. 50; *see also* TikTok Br. 17-20; Firebaugh Br. 16, 42. Statutes need not be backed by an administrative record, and "[n]either due process nor the First Amendment requires legislation to be supported by committee reports, floor debates, or even consideration, but only by a vote." *Time Warner Entm't Co. v. FCC*, 93 F.3d 957, 976 (D.C. Cir. 1996) (per curiam) (alteration in original) (quoting *Sable Commc'ns of Cal., Inc. v. FCC*, 492 U.S. 115, 133 (1989) (Scalia, J., concurring)).

1. The Act is content neutral because it does not draw "distinctions based on the message a speaker conveys." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). The restriction on TikTok's ownership reflects the considered judgment of the political branches that China has the capability and incentive to use the

application to amass massive amounts of U.S. user data and to exert covert influence over U.S. affairs in direct contravention of U.S. interests. As petitioners acknowledge, content on TikTok encompasses "all manner of topics, from sports and entertainment to religion and politics." TikTok Br. 5. The Act does not pick and choose among those topics and therefore does not implicate the same types of concerns as a law that "singles out specific subject matter for differential treatment." *Reed*, 576 U.S. at 169.

Nor does the Act prohibit or require any particular type of content moderation. Instead, the unique concern is that, due to a company's foreign ownership, a hostile foreign nation could use it to advance its own interests to the detriment of the United States. If a company without the same ties to a foreign adversary developed the same recommendation algorithm—or, indeed, acquired the algorithm currently used by TikTok, as expressly authorized by the statute—the Act would not apply. The statute's application to TikTok thus does not reflect any discrimination based on content or viewpoint, but rather the national-security risks described above. And the statute's provisions allowing regulation of other applications are likewise content neutral. The Act applies not to applications that provide any particular sort of content, but rather to a "foreign adversary controlled application," Act § 2(a)(1), which is defined in terms of ownership rather than content. In particular, the President has authority to designate other applications

that are "controlled by a foreign adversary" (China, Russia, North Korea, or Iran) and that "present a significant threat to the national security of the United States." Act § 2(g)(3)(B). Accordingly, the Act's prohibitions apply irrespective of whether the "viewpoints" expressed in videos on the application are predominately pro-American or anti-American. Firebaugh Br. 47. The Act targets situations where, as in the case of TikTok, a company that can be expected to follow one of those foreign adversaries' laws or directions operates an application implicating substantial national-security concerns.

Petitioners misunderstand the import of the statute's exception for applications "whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." Act § 2(g)(2)(B). Various businesses that sell products and services may have applications that allow users to post content of this kind—and that therefore technically satisfy the statute's definitions—but that would not share the unique attributes of dynamic platforms where users engage by sharing "text, images, videos, real-time communications, or similar content" for consumption by other users. Act § 2(g)(2)(A)(i). The Act does not express a preference for speech about "products, business, and travel" over speech about "politics, religion, and entertainment," TikTok Br. 36-37, but instead recognizes particular susceptibilities that arise from the manner that users interact and engage with social-media platforms like TikTok and similar websites.

Petitioners also misunderstand how the exception operates. The Act excludes from its reach "an entity that operates [an application] whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." Act § 2(g)(2)(B). The most natural reading of that language is that the listed review applications cannot serve as qualifying applications that subject a company to the Act's strictures, rather than that Congress created a loophole allowing otherwise-covered companies to escape regulation merely by also creating a review application. At a minimum, that understanding is a "plausible statutory construction[]" that "should prevail" over any construction that raises constitutional concerns. *Clark v. Martinez*, 543 U.S. 371, 380-81 (2005). And as petitioners' own precedent instructs, Firebaugh Br. 45-46, the correct remedy for any constitutional infirmity would be to sever the exception, not to invalidate the entire Act. *See Barr v. American Ass'n of Political Consultants, Inc.*, 591 U.S. 610, 636 (2020) (plurality opinion). That is particularly so where the exception applies only to entities that might be designated in the future (thus rendering it inapplicable to petitioners' claims), and where the statute has an express severability clause, *see* Act § 2(e).

Unable to locate any content-based distinctions in the statutory text, petitioners resort to conjecture about "the purpose and justification for the law." TikTok Br. 37 (quoting *Reed*, 576 U.S. at 166); Firebaugh Br. 46; BASED Br. 17.

But they overlook that the Act "serves purposes unrelated to the content of expression." *Ward*, 491 U.S. at 791. As discussed above, the Act is directed at preventing widespread data collection and covert malicious manipulation by foreign actors whose aims are antithetical to U.S. national-security interests. The Department of Justice's talking points and the House Committee on Energy and Commerce's report repeatedly emphasized those content-neutral objectives divorced from any suppression of free expression. *See* App.2 (describing how China has undermined U.S. "national security interests" by "us[ing] access to Americans' data" to "conduct espionage activities" and by "us[ing] deceptive and coercive methods to shape global information" (quotations omitted)); App.156 (discussing the "key national security concerns" that "TikTok collects tremendous amounts of sensitive data" and that China may "influence content on TikTok—without United States visibility"). Those goals are controlling "even if [the Act] has an incidental effect on some speakers or messages but not others." *Ward*, 491 U.S. at 791.

Petitioners seek to assign a different motive to Congress based largely on scattered statements by individual legislators, which they attribute to concerns about the platform's content rather than the actual concern about manipulation of the platform (including its content) by a foreign power. *See* TikTok Br. 19-21, 37-38; Firebaugh Br. 46-47. The Supreme Court "eschew[s]" this type of "guesswork"

when judging the constitutionality of a federal statute precisely because "[w]hat motivates one legislator to make a speech about a statute is not necessarily what motivates scores of others to enact it." *O'Brien*, 391 U.S. at 384. Petitioners' contentions underscore the hazards of asking a court "to void a statute that is, under well-settled criteria, constitutional on its face, on the basis of what fewer than a handful of Congressmen said about it." *Id.*

Moreover, in identifying some statements, petitioners fail to mention other probative legislative statements about the Act's content-neutral justifications. To take a non-exhaustive sample, legislators stated that the Act protects against foreign adversaries amassing "vast amounts of personal data from Americans" that "can be used to control or influence each of us," App.107; addresses the documented risk that content can "be covertly manipulated to serve the goals of an authoritarian regime," App.118; and "safeguard[s] our democratic systems from covert foreign influence, both in its application to TikTok and . . . future online platforms," App.121. More broadly, the consistent thread through discussion of the bill, reflected in the text of the enacted statute, *see* Act § 2(g)(3)(B) (defining covered applications based on whether they "present a significant threat to the national security of the United States"), was the national-security threat posed by a foreign adversary's ability to engage in nefarious data collection and covert influence.

Petitioners' claim that the Act draws an impermissible "speaker-based" distinction likewise fails. TikTok Br. 34-35; Firebaugh Br. 44. Again, the Act focuses on those applications whose foreign ownership and control raise national-security concerns, not on the identity of any speaker. And with respect to the Act's provisions at issue here, the Chinese government, using an algorithm in its own territory and subject to its control, has no First Amendment right as a "speaker" to project its hostile efforts into the United States. Regardless, speaker-based distinctions have been deemed problematic only "when the legislature's speaker preference reflects a content preference." *Reed*, 576 U.S. at 170 (quotation omitted). As explained at length above, the Act is not "simply a means to control content," which would call for heightened scrutiny. *Citizens United v. FEC*, 558 U.S. 310, 340 (2010).

2. Petitioners fare no better in suggesting that the statute is underinclusive. The "First Amendment imposes no freestanding 'underinclusiveness limitation.'" *Wagner v. FEC*, 793 F.3d 1, 27 (D.C. Cir. 2015) (en banc) (quoting *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 449 (2015)). Rather, "the primary purpose of underinclusiveness analysis is simply to ensure that the proffered state interest actually underlies the law" and to assess whether the law fails "to advance any genuinely substantial governmental interest" by "provid[ing] only ineffective or

remote support for the asserted goals." *National Ass'n of Mfrs. v. Taylor*, 582 F.3d 1, 17 (D.C. Cir. 2009) (quotations omitted).

As discussed above, the Act's application to TikTok has the purpose and effect of supporting Congress's national-security goals, regardless of whether additional entities may be designated in the future. Thus, even if Congress had limited the legislation to TikTok alone, the legislation would not be underinclusive. Congress "need not address all aspects of a problem in one fell swoop; policymakers may focus on their most pressing concerns," and such statutes are properly upheld "even under strict scrutiny." *Williams-Yulee*, 575 U.S. at 449.

Here, Congress had substantial information regarding the unique and serious threats posed by TikTok. *See supra* Part I. It thus sensibly addressed that pressing problem directly, while also empowering the Executive Branch to address similar threats in the future by authorizing the President to designate additional companies that "present a significant threat to the national security of the United States." Act § 2(g)(3)(B). It is hard to see how such additional authority, regardless of its limitations, could render the statute underinclusive. And those provisions, too, focus on a particular type of threat to national security and not on content or viewpoint. For example, the Act applies to account-based applications with over 1,000,000 monthly active users where users can both "generate or distribute content" of their own and "view content" made by others. Act § 2(g)(2)(A). The

potential for data collection and surreptitious content manipulation associated with such applications poses unique national-security risks that Congress was entitled to address, and Congress was under no obligation to simultaneously address smaller platforms or those that merely allow American users to view content and thus do not involve the same types of data or manipulable compilations of expression. Petitioners repeatedly ignore the ways in which "foreign ownership and control over [a social-media platform's] content-moderation decisions," *NetChoice*, 144 S. Ct. at 2410 (Barrett, J., concurring), can enable stealth campaigns to undercut U.S. national-security interests.

In any event, Congress simultaneously addressed other data-collection concerns at the same time it enacted the Act. In the same legislation, Congress enacted the Protecting Americans' Data from Foreign Adversaries Act, which prohibits "data broker[s]" from "mak[ing] available personally identifiable sensitive data of a United States individual" to foreign adversaries—including China—and any entity controlled by foreign adversaries. Pub. L. No. 118-50, div. I, § 2(a), 2(c)(3)-(5), 138 Stat. 960, 960-62 (2024). Nothing in Congress's two-part approach suggests that its desire to combat national-security risks was insincere or ineffective.

Nor are the Firebaugh petitioners correct in asserting that the statute is overbroad. Firebaugh Br. 60-62. The statute is not aimed at combatting some

specific expression on the platform, such that it could be overbroad as applied to other expression. Rather, the platform itself, as a whole and as currently operated, creates unacceptable national-security risk—at least so long as it remains subject to China's control. No narrower statute would address that problem.

3. The TikTok petitioners' invocation of equal-protection principles, *see* TikTok Br. 39-40, adds nothing to the analysis. The Supreme Court and this Court have long recognized that the sorts of First Amendment and equal-protection claims raised here involve "closely related" standards where "the critical questions asked are the same": whether the government action is appropriately tailored to serve a sufficiently strong interest. *Community-Service Broad. of Mid-America, Inc. v. FEC*, 593 F.2d 1102, 1122-23 (D.C. Cir. 1978) (en banc). The Act passes muster under that framework. *See supra* Part I.

In any event, the TikTok petitioners have not shown that they are the subject of unconstitutionally differential treatment. The Act creates a designation process to identify applications operated by an entity subject to certain foreign ownership or direction that are "determined by the President to present a significant threat to the national security of the United States." Act § 2(g)(3)(B). In the case of ByteDance and TikTok, Congress had a robust record to make the determination that those criteria were satisfied. *See, e.g.*, App.7-12 (summarizing many congressional proceedings related to the threats TikTok poses); *supra* Part I. Thus,

the statute itself designates ByteDance and TikTok as covered companies subject to the Act's prohibitions. Act § 2(g)(3)(A). ByteDance and TikTok in turn have exercised their right to bring a challenge to the Act. Act § 3.

The TikTok petitioners have already received all the process, and more, that would be afforded to other potentially regulated entities. *But see* TikTok Br. 42-43. Under the Act, applications other than TikTok may be designated "following the issuance" of "a public notice" and "a public report to Congress . . . describing the specific national security concern involved and containing a classified annex and a description of what assets would need to be divested." Act § 2(g)(3)(B)(ii). Over the last four years, the Executive Branch took formal action against TikTok twice, and there have been numerous public and classified hearings and briefings, extensive reports, and a comprehensive back-and-forth between TikTok and the Executive Branch about national-security concerns and possible ameliorative measures. *See* Newman Decl. ¶¶36-48 (summarizing negotiations over a proposed national security agreement). By its own account, TikTok has engaged in "multi-year efforts" to assuage the government's concerns. TikTok Br. 2.

4. For similar reasons, there is no merit to the TikTok petitioners' suggestion that "[i]t is not yet apparent how the government will seek to defend the Act" and that the government's national-security rationales constitute "post hoc justifications." TikTok Br. 71. As noted, *see supra* p. 66, statutes need not be

accompanied by an administrative record for judicial review. Regardless, the serious national-security concerns that Congress sought to address are plain from the public record and the course of dealing with the company. And the TikTok petitioners' cursory suggestion that the government should be foreclosed from relying on classified material ignores binding precedent that "the court has inherent authority to review classified material *ex parte*, *in camera* as part of its judicial review function." *Jifry v. FAA*, 370 F.3d 1174, 1182 (D.C. Cir. 2004). This Court has expressly rejected the argument that the petitioners could not "defend against the charge that they are security risks" without knowledge of specific classified information upon which the government relied. *Id.* at 1184.

5. The Firebaugh petitioners make no headway in attempting to recast the Act as infringing the rights to associate and receive information. Firebaugh Br. 30-35. It is difficult to see how this case implicates associational rights at all. The paradigmatic cases involve laws that "directly interfere with an organization's composition" or "ma[k]e group membership less attractive." *Rumsfeld v. Forum for Acad. & Institutional Rights, Inc.*, 547 U.S. 47, 69 (2006); *see also Americans for Prosperity Found. v. Bonta*, 594 U.S. 595, 606 (2021) (listing examples "where a group is required to take in members it does not want" and "where members of an organization are denied benefits based on the organization's message"). Here, petitioners focus their arguments on the ability to "associate" with TikTok itself.

But those arguments do not—and cannot—establish that petitioners are part of a group whose "ability to express its message" is inhibited by the Act. *Forum for Acad. & Institutional Rights*, 547 U.S. at 69. Petitioners' assertions (Firebaugh Br. 30-33, 63; BASED Br. 4-9, 24-25) largely boil down to the notion that they "would prefer to affiliate" with TikTok as an editor and publisher, but they "cannot export their own First Amendment rights" in this way. *Agency for Int'l Dev.*, 591 U.S. at 437-38.

As to the right to receive information, even for purposes of standing—much less a substantive First Amendment claim—the Supreme Court has recognized a "cognizable injury only where the listener has a concrete, specific connection to the speaker." *Murthy v. Missouri*, 144 S. Ct. 1972, 1996 (2024). Petitioners' general desire to consume content on TikTok does not qualify.

In addition, petitioners' arguments in support of their asserted rights as listeners suffer from all the same flaws as their arguments in support of their rights as content creators. The statute has neither the purpose nor effect of preventing foreign entities from expressing certain views, which can be freely disseminated in any forum other than the platform that has given rise to national-security risks in light of its ownership. This case thus bears no resemblance to *Lamont v. Postmaster General*, 381 U.S. 301 (1965), where the Supreme Court invalidated a statute that restricted the delivery through the Postal Service of mail deemed

"communist political propaganda," *id.* at 302. *Cf. Trump v. Hawaii*, 585 U.S. 667, 703 (2018) (noting that limitations on Americans' "right to receive information" from foreign actors may be appropriate where "the Executive gave a facially legitimate and bona fide reason for its action" (quotations omitted)).

6. The Firebaugh and BASED petitioners fundamentally misunderstand the relevant doctrine when they compare the Act to a prior restraint on speech on the ground that it "forbids communications before they occur, banning them as unlawful regardless of their content." Firebaugh Br. 38; *see also* BASED Br. 15-17. On this theory, any time, place, and manner restriction would be a prior restraint to the extent that it categorically prohibited speech in a particular location. The fact that the Act does not depend on the content of speech is a constitutional virtue, not a vice. And the Act does not contemplate an injunction against speech like the provision invalidated in *Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931), but rather after-the-fact enforcement in the form of civil penalties or an injunction against the non-speech activities that the Act actually prohibits. *See* Act § 2(a), (d).

Prior restraints are problematic because they raise the specter that officials will exercise "unconfined authority to pass judgment on the content of speech" as a means of stifling disfavored speech or speakers. *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 320 (2002). The Act presents no such concerns.

III. The TikTok Petitioners' Fallback Constitutional Arguments Are Meritless

A. The Act Is Not a Bill of Attainder

The Act is not an unconstitutional bill of attainder under Article I, Section 9 of the Constitution for two independent reasons: the Act does not impose the sort of legislative punishment proscribed by the Bill of Attainder Clause, and the Clause does not apply to corporate entities like ByteDance and TikTok in any event. The Clause prohibits Congress from enacting laws "that legislatively determine[] guilt and inflict[] punishment upon an identifiable individual without provision of the protections of a judicial trial." *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 468 (1977).

1. As the TikTok petitioners appear to acknowledge, TikTok Br. 62, it is not enough that the Act "refers to" ByteDance and TikTok "by name," *Nixon*, 433 U.S. at 471-72. A law is not unconstitutional simply because it "burdens some persons or groups but not all other plausible individuals." *Id.* at 471. Instead, the central task is to "distinguish permissible burdens from impermissible punishments." *Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec.*, 909 F.3d 446, 455 (D.C. Cir. 2018).

The "most important" consideration is "whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *Kaspersky Lab*, 909 F.3d at 455 (quotations

omitted). Here, the nonpunitive interests supporting the Act are apparent: there are substantial national-security concerns with China's ability to use TikTok to gain access to vast stores of U.S. user data and to engage in covert foreign influence.

The Act's scope further underscores its nonpunitive nature. The Act covers not only TikTok but also other foreign adversary controlled applications that are determined to "present a significant threat to the national security of the United States." Act § 2(g)(3)(B). That the Executive Branch and Congress had a sufficiently robust record to make that evaluation at the time of enactment as to TikTok does not undermine the Act's legitimate nonpunitive objectives. The TikTok petitioners repeatedly seek to draw an inapt comparison to a statute that "singl[ed] out [the appellant] as virtually the only [person] subject to the [law]." *Foretich v. United States*, 351 F.3d 1198, 1223 (D.C. Cir. 2003). By contrast, the Act is not so narrowly circumscribed as to target one entity or group with a burden "so disproportionate" as to suggest that the Act is "an end in and of itself" rather than "a means to an end." *Kaspersky Lab*, 909 F.3d at 455.

The TikTok petitioners' "failure to raise a suspicion of punitiveness under the functional test" is virtually dispositive, but they also have not made "a persuasive showing" under either of the other tests for identifying bills of attainder. *Kaspersky Lab*, 909 F.3d at 460. The Act does not resemble the "ready checklist of deprivations and disabilities" that historically have been understood "to fall within

the proscription," such as a criminal sentence or the seizure of property. *Nixon*, 433 U.S. at 473, 474 n.38; *Kaspersky Lab*, 909 F.3d at 460. Rather, the statute targets the precise harm Congress was concerned about—control by a foreign adversary—and permits TikTok to continue operating without penalty if Chinese control is removed. This Court has made clear that "the Bill of Attainder Clause tolerates statutes that" prevent regulated entities "from engaging in particular kinds of business or particular combinations of business endeavors." *Kaspersky Lab*, 909 F.3d at 463. The Act is precisely such a regulation aimed at addressing national-security concerns resulting from foreign ownership and control.

Petitioners likewise have not identified "unmistakable evidence of punitive intent." *Foretich*, 351 F.3d at 1225 (quotation omitted). As explained above, Congress overwhelmingly voted in favor of the Act based on specific data-collection and content-manipulation concerns. Any perceived difference in treatment between TikTok and other applications in the Act is not indicative of a congressional desire to punish but instead to address a substantiated potential threat that demands prompt attention.

2. Regardless, the Clause does not apply to corporations as opposed to natural persons. Neither the Supreme Court nor this Court has applied the Clause in that context. *See Kaspersky Lab*, 909 F.3d at 454 (assuming without deciding the issue). The Supreme Court has made clear that the Clause concerns "legislative

interferences[] in cases affecting personal rights," *United States v. Brown*, 381 U.S. 437, 444 n.18 (1965) (quoting *The Federalist*, No. 44, at 351 (James Madison) (Hamilton ed. 1880)), and operates "only as [a] protection[] for individual persons and private groups," *South Carolina v. Katzenbach*, 383 U.S. 301, 324 (1966).

And historically, an attainder was understood as "the act of extinguishing a person's civil rights when that person is sentenced to death or declared an outlaw for committing a felony or treason." *Attainder*, Black's Law Dictionary (12th ed. 2024). In describing the "infamous history of bills of attainder" that led to the Clause's adoption, the Supreme Court cited numerous historical examples of acts imposing punishments—including death, imprisonment, banishment, and confiscation of property—on natural persons. *Nixon*, 433 U.S. at 473-74 & nn.35-38; *see also Brown*, 381 U.S. at 441-42 & nn.10-12 (reciting other examples). Extending the Clause to allow large corporations to relieve themselves of regulatory burdens would not serve the animating purposes of protecting "those who are peculiarly vulnerable" from retribution for political beliefs. *Katzenbach*, 383 U.S. at 324. That is especially so for a foreign-controlled corporation presenting a threat to national security by a foreign adversary.

B. The Act Does Not Effect a Taking

The TikTok petitioners briefly argue (at 68-70) that the Act effects a taking. This cursory argument is meritless.

As an initial matter, the TikTok petitioners properly neither contend that the Act effectuates a "physical appropriation[]" of property nor invoke the balancing test generally applied to claims that a regulation improperly "restrict[s] an owner's ability to use his own property" in certain ways without compensation. *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 147-48 (2021). Instead, they argue only that the Act is a per se taking because it deprives them of *all* economically beneficial use of their property. But there can be no serious dispute that TikTok US and ByteDance have assets that can be sold. Those assets include not only the billions of lines of code that underlie the TikTok application and the application's value as an ongoing business even without access to features like the algorithm (captured in, for example, the application's large established user base, its brand value, and its goodwill) but also all the additional property the companies may own. The TikTok petitioners have failed to substantiate their contention that these assets have no economic value independent of the algorithm. The declaration cited does not suggest otherwise, merely contending that the Act would prevent the mobile application from functioning in the United States. *See* App.824-27. Nor have petitioners adduced evidence of an unsuccessful effort to sell the platform for value.

Even as to the application itself, the Act does not prohibit TikTok's continued use but merely requires divestment from its China-based owner,

ByteDance. The possibility that Chinese law, or other practical impediments, may require TikTok to alter its algorithm or otherwise modify the business when ByteDance divests in no way allows petitioners to demonstrate that their business has been entirely eliminated—much less that *the Act* caused such an elimination.

The TikTok petitioners largely rely on cases in which the government restricted or eliminated the uses of tangible property—typically real property—in a way that could not be counteracted through sale or other measures. Even in that context, the requirement that the challenger demonstrate that all economic value be eliminated has been strictly observed. *See Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 125-28 (1978) (citing cases in which severe restrictions on the use of property were not held to be takings). As the Supreme Court has explained, "'taking' challenges have . . . been held to be without merit in a wide variety of situations when the challenged governmental actions prohibited a beneficial use to which individual parcels had previously been devoted and thus caused substantial individualized harm." *Id.* at 125.

The fact that this case involves not real property, or even personal property, but an intangible business even further weakens petitioners' argument. The only case they cite involving a business, *Kimball Laundry Co. v. United States*, 338 U.S. 1 (1949), involved a dispute about how to calculate the compensation when the government had appropriated a business for government use during a war. It

provides no support for the proposition that regulations of businesses to support legitimate governmental objectives constitute a taking.

IV. Petitioners Are Not Entitled to an Injunction

Because petitioners' claims are meritless, no injunction is warranted. *See Sherley v. Sebelius*, 644 F.3d 388, 398 (D.C. Cir. 2011). Regardless, as amply demonstrated, *see supra* Part I, TikTok's continued operation in the United States poses substantial harms to national security by virtue of TikTok's data-collection practices and the intelligence and surveillance efforts of the Chinese government—harms that equally run against the public interest. *Nken v. Holder*, 556 U.S. 418, 435 (2009). Congress determined that ByteDance's ownership of TikTok poses an unacceptable risk to national security because that corporate relationship could permit the Chinese government to collect intelligence on and manipulate the content received by TikTok's American users. That risk assessment is "entitled to deference," *Humanitarian Law Project*, 561 U.S. at 33, and the Supreme Court has cautioned against "[j]udicial inquiry" into issues of national security that are the "constitutional responsibilit[y]" of the political branches, *Trump*, 585 U.S. at 704 (first alteration in original) (quotation omitted). Thus, even assuming that petitioners had met their "high standard" for establishing irreparable injury, *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006), the balance of the equities and the public interest would counsel against

injunctive relief. *Cf. eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 391-94 (2006).

Nor should the Court entertain petitioners' brief alternative suggestion that they are entitled to a preliminary injunction and unspecified "further proceedings" if "the Court were to find genuine issues of material fact that preclude judgment" on this record. TikTok Br. 72; *see also* Firebaugh Br. 66; BASED Br. 28-30. Having agreed to permit each side to present its factual submissions in connection with legal briefs, *see* Joint Mot. to Set Briefing and Oral Argument Schedule (May 17, 2024), petitioners have no basis for requesting additional procedures. Much less can petitioners justify their suggestion that they receive the "extraordinary remedy" of a preliminary injunction in the meantime. *Chaplaincy of Full Gospel Churches*, 454 F.3d at 297 (quotation omitted).

Finally, as petitioners implicitly concede, any relief must be narrowly circumscribed to apply only to the provisions of the Act that the Court finds unlawful. The Act itself contains an express severability clause, *see* Act § 2(e), and giving effect to that clause comports with the "normal rule" that courts must "limit the solution to the problem, severing any problematic portions while leaving the remainder intact." *Association of Am. R.Rs. v. U.S. Dep't of Transp.*, 896 F.3d 539, 549 (D.C. Cir. 2018) (quotations omitted). Thus, in particular, because petitioners challenge only the Act's provisions that apply directly to ByteDance and TikTok,

any injunction must be limited to those provisions and, in particular, should not enjoin the enforcement of the Act's separate pathway for Executive designation. Nevertheless, the government agrees with the TikTok petitioners' contention (at 72) that Section 2(b) should not take effect if the Attorney General is enjoined from enforcing Section 2(a) as applied to TikTok and ByteDance. Petitioners' rationale that the provision is non-severable is incorrect, *see* Act § 2(e), but by its terms, Section 2(b) does not take effect until "subsection (a) applies to a foreign adversary controlled application," Act § 2(b). That would not occur if enforcement of subsection (a) were enjoined as applied to TikTok.

CONCLUSION

For the foregoing reasons, the petitions for review should be denied.

Respectfully submitted,

TRICIA WELLMAN
Acting General Counsel
JAMES R. POWERS
Chief, Litigation
JENNIFER M. PIKE
Associate General Counsel
Office of the Director of National Intelligence

DIANE KELLEHER
BONNIE E. DEVANY
SIMON G. JEROME
Attorneys, Federal Programs Branch
Civil Division
U.S. Department of Justice

MATTHEW G. OLSEN
Assistant Attorney General for National Security
DEVIN A. DEBACKER
Chief, Foreign Investment Review Section
ERIC S. JOHNSON
Principal Deputy Chief, Foreign Investment Review Section
TYLER J. WOOD
Deputy Chief, Foreign Investment Review Section
EVAN SILLS
Attorney-Advisor, Foreign Investment Review Section
National Security Division
U.S. Department of Justice

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

BRIAN D. NETTER
Deputy Assistant Attorney General

MARK R. FREEMAN
SHARON SWINGLE
DANIEL TENNY
CASEN B. ROSS

/s/ Sean R. Janda
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys, Appellate Staff
Civil Division, Room 7260
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-3388
sean.r.janda@usdoj.gov

BRADLEY BOOKER
General Counsel
KELLY SMITH
Section Chief
NADIN LINTHORST
Assistant General Counsel
TUCKER MCNULTY
Assistant General Counsel
ANN OAKES
Assistant General Counsel
Federal Bureau of Investigation

July 2024

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of this Court's order of May 28, 2024 because it contains 19,397 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Word for Microsoft 365 in Calisto MT 14-point font, a proportionally spaced typeface.

/s/ Sean R. Janda
Sean R. Janda

CERTIFICATE OF SERVICE

I hereby certify that on July 26, 2024, I filed the unredacted, classified version of this brief by causing an original and three copies to be lodged with the Department of Justice Classified Information Security Officer. I further certify that on July 26, 2024, I electronically filed the public, unclassified version of this brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. Service on all parties will be accomplished by the appellate CM/ECF system.

/s/ Sean R. Janda
Sean R. Janda

ADDENDUM

TABLE OF CONTENTS

Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H (2024)

§ 1. SHORT TITLE.

This division may be cited as the "Protecting Americans from Foreign Adversary Controlled Applications Act".

§ 2. PROHIBITION OF FOREIGN ADVERSARY CONTROLLED APPLICATIONS.

(a) IN GENERAL.—

(1) PROHIBITION OF FOREIGN ADVERSARY CONTROLLED APPLICATIONS.—It shall be unlawful for an entity to distribute, maintain, or update (or enable the distribution, maintenance, or updating of) a foreign adversary controlled application by carrying out, within the land or maritime borders of the United States, any of the following:

(A) Providing services to distribute, maintain, or update such foreign adversary controlled application (including any source code of such application) by means of a marketplace (including an online mobile application store) through which users within the land or maritime borders of the United States may access, maintain, or update such application.

(B) Providing internet hosting services to enable the distribution, maintenance, or updating of such foreign adversary controlled application for users within the land or maritime borders of the United States.

(2) APPLICABILITY.—Subject to paragraph (3), this subsection shall apply—

(A) in the case of an application that satisfies the definition of a foreign adversary controlled application pursuant to subsection (g)(3)(A), beginning on the date that is 270 days after the date of the enactment of this division; and

(B) in the case of an application that satisfies the definition of a foreign adversary controlled application pursuant to subsection (g)(3)(B), beginning on the date that is 270 days after the date of the relevant determination of the President under such subsection.

(3) EXTENSION.—With respect to a foreign adversary controlled application, the President may grant a 1-time extension of not more than 90 days with respect to the date on which this subsection would otherwise apply to such application pursuant to paragraph (2), if the President certifies to Congress that—

(A) a path to executing a qualified divestiture has been identified with respect to such application;

(B) evidence of significant progress toward executing such qualified divestiture has been produced with respect to such application; and

(C) there are in place the relevant binding legal agreements to enable execution of such qualified divestiture during the period of such extension.

(b) DATA AND INFORMATION PORTABILITY TO ALTERNATIVE APPLICATIONS.—Before the date on which a prohibition under subsection (a) applies to a foreign adversary controlled application, the entity that owns or controls such application shall provide, upon request by a user of such application within the land or maritime borders of United States, to such user all the available data related to the account of such user with respect to such application. Such data shall be provided in a machine readable format and shall include any data maintained by such application with respect to the account of such user, including content (including posts, photos, and videos) and all other account information.

(c) EXEMPTIONS.—

(1) EXEMPTIONS FOR QUALIFIED DIVESTITURES.—Subsection (a)—

(A) does not apply to a foreign adversary controlled application with respect to which a qualified divestiture is executed before the date on which a prohibition under subsection (a) would begin to apply to such application; and

(B) shall cease to apply in the case of a foreign adversary controlled application with respect to which a qualified divestiture is executed after the date on which a prohibition under subsection (a) applies to such application.

(2) EXEMPTIONS FOR CERTAIN NECESSARY SERVICES.—Subsections (a) and (b) do not apply to services provided with respect to a foreign adversary controlled application that are necessary for an entity to attain compliance with such subsections.

(d) ENFORCEMENT.—

(1) CIVIL PENALTIES.—

(A) FOREIGN ADVERSARY CONTROLLED APPLICATION VIOLATIONS.—An entity that violates subsection (a) shall be subject to pay a civil penalty in an amount not to exceed the amount that results from multiplying $5,000 by the number of users within the land or maritime borders of the United States determined to have accessed, maintained, or updated a foreign adversary controlled application as a result of such violation.

(B) DATA AND INFORMATION VIOLATIONS.—An entity that violates subsection (b) shall be subject to pay a civil penalty in an amount not to exceed the amount that results from multiplying $500 by the number of users within the land or maritime borders of the United States affected by such violation.

(2) ACTIONS BY ATTORNEY GENERAL.—The Attorney General—

(A) shall conduct investigations related to potential violations of subsection (a) or (b), and, if such an investigation results in a determination that a violation has occurred, the Attorney General shall pursue enforcement under paragraph (1); and

(B) may bring an action in an appropriate district court of the United States for appropriate relief, including civil penalties under paragraph (1) or declaratory and injunctive relief.

(e) SEVERABILITY.—

(1) IN GENERAL.—If any provision of this section or the application of this section to any person or circumstance is held invalid, the invalidity shall not affect the other provisions or applications of this section that can be given effect without the invalid provision or application.

(2) SUBSEQUENT DETERMINATIONS.—If the application of any provision of this section is held invalid with respect to a foreign adversary controlled application that satisfies the definition of such term pursuant to subsection (g)(3)(A), such invalidity shall not affect or preclude the application of the same provision of this section to such foreign adversary controlled application by means of a subsequent determination pursuant to subsection (g)(3)(B).

(f) RULE OF CONSTRUCTION.—Nothing in this division may be construed—

(1) to authorize the Attorney General to pursue enforcement, under this section, other than enforcement of subsection (a) or (b);

(2) to authorize the Attorney General to pursue enforcement, under this section, against an individual user of a foreign adversary controlled application; or

(3) except as expressly provided herein, to alter or affect any other authority provided by or established under another provision of Federal law.

(g) DEFINITIONS.—In this section:

(1) CONTROLLED BY A FOREIGN ADVERSARY.—The term "controlled by a foreign adversary" means, with respect to a covered company or other entity, that such company or other entity is—

(A) a foreign person that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country;

(B) an entity with respect to which a foreign person or combination of foreign persons described in subparagraph (A) directly or indirectly own at least a 20 percent stake; or

(C) a person subject to the direction or control of a foreign person or entity described in subparagraph (A) or (B).

(2) COVERED COMPANY.—

(A) IN GENERAL.—The term "covered company" means an entity that operates, directly or indirectly (including through a parent company, subsidiary, or affiliate), a website, desktop application, mobile application, or augmented or immersive technology application that—

(i) permits a user to create an account or profile to generate, share, and view text, images, videos, real-time communications, or similar content;

(ii) has more than 1,000,000 monthly active users with respect to at least 2 of the 3 months preceding the date on which a relevant determination of the President is made pursuant to paragraph (3)(B);

(iii) enables 1 or more users to generate or distribute content that can be viewed by other users of the website, desktop application, mobile application, or augmented or immersive technology application; and

(iv) enables 1 or more users to view content generated by other users of the website, desktop application, mobile application, or augmented or immersive technology application.

(B) EXCLUSION.—The term "covered company" does not include an entity that operates a website, desktop application, mobile application, or augmented or immersive technology application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.

(3) FOREIGN ADVERSARY CONTROLLED APPLICATION.—The term "foreign adversary controlled application" means a website, desktop application, mobile application, or augmented or immersive technology application that is operated, directly or indirectly (including through a parent company, subsidiary, or affiliate), by—

(A) any of—

(i) ByteDance, Ltd.;

(ii) TikTok;

(iii) a subsidiary of or a successor to an entity identified in clause (i) or (ii) that is controlled by a foreign adversary; or

(iv) an entity owned or controlled, directly or indirectly, by an entity identified in clause (i), (ii), or (iii); or

(B) a covered company that—

(i) is controlled by a foreign adversary; and

(ii) that is determined by the President to present a significant threat to the national security of the United States following the issuance of—

(I) a public notice proposing such determination; and

(II) a public report to Congress, submitted not less than 30 days before such determination, describing the specific national security concern involved and containing a classified annex and a description of what assets would need to be divested to execute a qualified divestiture.

(4) FOREIGN ADVERSARY COUNTRY.—The term "foreign adversary country" means a country specified in section 4872(d)(2) of title 10, United States Code.

(5) INTERNET HOSTING SERVICE.—The term "internet hosting service" means a service through which storage and computing resources are provided to an individual or organization for the accommodation and maintenance of 1 or more websites or online services, and which may include file hosting, domain name server hosting, cloud hosting, and virtual private server hosting.

(6) QUALIFIED DIVESTITURE.—The term "qualified divestiture" means a divestiture or similar transaction that—

(A) the President determines, through an interagency process, would result in the relevant foreign adversary controlled application no longer being controlled by a foreign adversary; and

(B) the President determines, through an interagency process, precludes the establishment or maintenance of any operational relationship between the United States operations of the relevant foreign adversary controlled application and any formerly affiliated entities that are controlled by a foreign adversary, including any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing.

(7) SOURCE CODE.—The term "source code" means the combination of text and other characters comprising the content, both viewable and nonviewable, of a software application, including any publishing language, programming language, protocol, or functional content, as well as any successor languages or protocols.

(8) UNITED STATES.—The term "United States" includes the territories of the United States.

§ 3. JUDICIAL REVIEW.

(a) RIGHT OF ACTION.—A petition for review challenging this division or any action, finding, or determination under this division may be filed only in the United States Court of Appeals for the District of Columbia Circuit.

(b) EXCLUSIVE JURISDICTION.—The United States Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over any challenge to this division or any action, finding, or determination under this division.

(c) STATUTE OF LIMITATIONS.—A challenge may only be brought—

(1) in the case of a challenge to this division, not later than 165 days after the date of the enactment of this division; and

(2) in the case of a challenge to any action, finding, or determination under this division, not later than 90 days after the date of such action, finding, or determination.