Nos. 24-656 and 24-657

In the Supreme Court of the United States

TIKTOK INC. AND BYTEDANCE LTD., PETITIONERS

v.

MERRICK B. GARLAND, ATTORNEY GENERAL

BRIAN FIREBAUGH, ET AL., PETITIONERS

v.

MERRICK B. GARLAND, ATTORNEY GENERAL

ON WRITS OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

BRIEF FOR THE RESPONDENT

ELIZABETH B. PRELOGAR
Solicitor General
Counsel of Record
BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
EDWIN S. KNEEDLER
Deputy Solicitor General
SOPAN JOSHI
Assistant to the Solicitor General
MARK R. FREEMAN
SHARON SWINGLE
DANIEL TENNY
CASEN B. ROSS
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the Protecting Americans from Foreign Adversary Controlled Applications Act, as applied to petitioners, violates the First Amendment.

PARTIES TO THE PROCEEDING

Petitioners in No. 24-656 (petitioners below) are TikTok Inc. and ByteDance Ltd.

Petitioners in No. 24-657 (also petitioners below) are Brian Firebaugh, Chloe Joy Sexton, Talia Cadet, Timothy Martin, Kiera Spann, Paul Tran, Christopher Townsend, Steven King, and BASED Politics, Inc.

Respondent in both cases (respondent below) is Merrick B. Garland, in his official capacity as Attorney General of the United States.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases: Page

Cases—Continued: Page

Cases—Continued: Page

Constitution, statutes, and regulations:

In the Supreme Court of the United States

No. 24-656

TIKTOK INC. AND BYTEDANCE LTD., PETITIONERS

v.

MERRICK B. GARLAND, ATTORNEY GENERAL

No. 24-657

BRIAN FIREBAUGH, ET AL., PETITIONERS

v.

MERRICK B. GARLAND, ATTORNEY GENERAL

ON WRITS OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

BRIEF FOR THE RESPONDENT

OPINION BELOW

The opinion of the court of appeals (J.A. 1-92) is available at 2024 WL 4996719.

JURISDICTION

The judgments of the court of appeals were entered on December 6, 2024. On December 18, 2024, this Court treated petitioners' applications for injunctions pending further review as petitions for writs of certiorari and granted the petitions. The jurisdiction of this Court rests on 28 U.S.C. 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The First Amendment provides in pertinent part that "Congress shall make no law * * * abridging the freedom of speech." U.S. Const. Amend. I.

The Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, Div. H, 138 Stat. 955, is reproduced in the appendix to this brief. App., *infra*, 1a-10a.

STATEMENT

This case concerns TikTok, a social-media platform subject to the control of the People's Republic of China (PRC)—a nation that Congress has deemed a foreign adversary of the United States. TikTok collects vast swaths of data about tens of millions of Americans, which the PRC could use for espionage or blackmail. And the PRC could covertly manipulate the platform to advance its geopolitical interests and harm the United States—by, for example, sowing discord and disinformation during a crisis. In response to those grave national-security threats, Congress did not impose any restriction on speech, much less one based on viewpoint or content. Instead, Congress restricted only *foreign adversary control*: TikTok may continue operating in the United States and presenting the same content from the same users in the same manner if its current owner executes a divestiture that frees the platform from the PRC's control. The question presented is whether that divestiture requirement violates the First Amendment.

A. TikTok, ByteDance, And The PRC

1. "TikTok is a social-media platform that lets users create, upload, and watch short video clips overlaid with text, voiceovers, and music." J.A. 8. TikTok has "ap-

proximately 170 million monthly users in the United States." *Ibid.* Petitioner TikTok Inc., a California company, "provides the TikTok platform to users in the United States," but that company is wholly owned through a chain of corporate entities by petitioner ByteDance Ltd., which "is the ultimate parent of TikTok." J.A. 8, 10. ByteDance is incorporated in the Cayman Islands, but it is headquartered in Beijing and "primarily operat[es] out of offices in the PRC." J.A. 637 (Blackburn Decl. ¶ 39); see J.A. 671-672 (Newman Decl. ¶ 9); J.A. 10; H.R. Rep. No. 417, 118th Cong., 2d Sess. 3 (2024) (House Report) (reprinted at J.A. 210-227).

"What a TikTok user sees on the platform is determined by a recommendation engine, company content moderation decisions, and video promotion and filtering decisions." J.A. 8. "TikTok's success rests in large part on its proprietary algorithm, owned by ByteDance and engineered and stored in the PRC, which drives the platform's Recommendation Engine." J.A. 673 (Newman Decl. ¶ 15). ByteDance "originally developed" the source code for the recommendation engine and remains responsible for developing "'computer code that runs the TikTok platform.'" J.A. 8, 10. The TikTok platform is thus "highly integrated with ByteDance." J.A. 10. And the PRC government has forbidden the export of the algorithm behind TikTok's recommendation engine. J.A. 64; see 24-1113 Pet. C.A. Br. 24; J.A. 649 (Blackburn Decl. ¶ 78).

"Because of the authoritarian structures and laws of the PRC regime, Chinese companies lack meaningful independence from the PRC's agenda and objectives." J.A. 673 (Newman Decl. ¶ 17). "As a result, even putatively 'private' companies based in China do not operate with independence from the government." *Ibid.* In-

deed, "the PRC maintains a powerful Chinese Communist Party committee 'embedded in ByteDance' through which it can 'exert its will on the company.'" J.A. 36; see *ibid.* (explaining that the committee includes "at least 138 employees," including ByteDance's "chief editor"). That interlinkage creates what is called a "hybrid commercial threat," J.A. 35, "a global phenomenon that allow[s] foreign governments—and the PRC in particular—to take advantage of legitimate business operations and leverage commercial access to pursue strategic national goals," J.A. 657 (Vorndran Decl. ¶ 6). The "PRC endeavors strategically to preposition commercial entities in the United States that the PRC can later 'co-opt'" when the time is ripe. J.A. 35.

2. Since TikTok was launched in 2017, it has generated significant national-security concerns across two presidential Administrations and in Congress. Those concerns are primarily grounded in two features of TikTok's operation, combined with ByteDance's "tight interlinkages" with the Chinese government and the Chinese Communist Party. J.A. 212 (House Report 3). Those aspects of TikTok's operation are of significant concern because the PRC actively seeks to "undercut U.S. influence, drive wedges between the United States and its partners, surpass the United States in comprehensive national power, and foster norms that favor the PRC's authoritarian system." J.A. 630 (Blackburn Decl. ¶ 16).

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 appli-

cation, and videos watched." J.A. 212 (House Report 3); see J.A. 659-662 (Vorndran Decl. ¶¶ 17-33). Chinese law generally requires Chinese companies to "assist or cooperate" with Chinese "intelligence work" and ensures that the PRC and its security agencies have "the power to access and control private data" held by those companies. J.A. 213 (House Report 4); see J.A. 673-676 (Newman Decl. ¶¶ 16-25) (describing several such laws). 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." Exec. Order No. 13,942, 85 Fed. Reg. 48,637, 48,637 (Aug. 11, 2020).

Second, because TikTok is integrated with ByteDance and relies on the proprietary engine developed and maintained in China, its corporate structure creates the risk that the Chinese government could covertly "control the recommendation algorithm, which could be used for influence operations." J.A. 217 (House Report 8) (citation omitted); see J.A. 647-649 (Blackburn Decl. ¶¶ 68-69, 71, 73, 76, 78). The PRC already has used social media to conduct "a campaign of harassment against pro-democracy dissidents in the United States." J.A. 633 (Blackburn Decl. ¶ 28). ByteDance also has "taken action in response to PRC demands to censor content *outside* of China" and has "a demonstrated history of manipulating the content on [TikTok], including at the direction of the PRC," J.A. 641, 644 (Blackburn Decl. ¶¶ 54, 58). Although the record does not reflect ByteDance's having taken such actions on TikTok in the

United States, the Executive Branch determined that "ByteDance and TikTok similarly would try to comply if the PRC asked for specific actions to be taken to manipulate content for censorship, propaganda, or other malign purposes on TikTok" in the United States. J.A. 647 (Blackburn Decl. ¶ 69). The PRC could use such covert content manipulation and distortion on TikTok to, among other things, "sow doubts about U.S. leadership," "undermine democracy," "counter other countries' policies that threaten the PRC's interests," and "magnify U.S. societal divisions in ways favorable to the PRC." J.A. 634 (Blackburn Decl. ¶ 29).

B. Previous Efforts To Address TikTok's Threat To National Security

Over the last four years, concerns about TikTok's threat to national security have prompted repeated Executive Branch and congressional action. 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." *Ibid.* The President concluded that TikTok's data collection posed a risk that the PRC and the Chinese Communist Party would have access to that data and use it for malign purposes, such as tracking the locations of U.S. persons, blackmail, and espionage. *Ibid.*

Invoking the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701 *et seq.*, 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 Executive Branch's authority under IEEPA. 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. Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 11, 2021).

Also in August 2020, President Trump ordered ByteDance to divest all interests and rights in any property used to support ByteDance's operation of TikTok in the United States and any data obtained or derived from TikTok's U.S. users. See 85 Fed. Reg. 51,297 (Aug. 19, 2020). That divestiture order followed a review by the Committee on Foreign Investment in the United States (CFIUS) of ByteDance's acquisition of the social-media platform Musical.ly. The divestiture order was challenged, see *TikTok* v. *CFIUS*, No. 20-1444 (D.C. Cir.), and it was not enforced in order to enable the parties to undertake discussions to explore whether they could identify an alternative resolution that would adequately mitigate the government's national-security concerns. See J.A. 678-681 (Newman Decl. ¶¶ 36-48).

Although the government engaged in several years of good-faith negotiations with ByteDance, the parties were unable to reach a resolution. "Executive Branch personnel in 2021 and 2022 reviewed dozens of proposed draft mitigation terms and held a series of meetings," which "frequently included extensive discussions driven

by subject matter experts in data storage, source code and software review, content review, lawful process, content moderation, and trust and safety." J.A. 680 (Newman Decl. ¶ 44). The government also "engaged in extensive, in-depth discussions with Oracle," which ByteDance had proposed would "stor[e] data in the United States" and "perform[] source code review." J.A. 680 (Newman Decl. ¶ 45). Ultimately, despite "dozens of meetings" and the exchange of "scores of drafts of proposed mitigation terms," senior Executive Branch officials determined that the "national security agreement" that ByteDance eventually proposed did not "sufficiently address the identified national security risks." J.A. 680-681 (Newman Decl. ¶¶ 47, 49); see J.A. 686 (Newman Decl. ¶ 75).

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." J.A. 218 (House Report 9); see No TikTok on Government Devices Act, Pub. L. No. 117-328, Div. R, 136 Stat. 5258. 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." J.A. 213 (House Report 4). A "majority of states" have likewise "banned TikTok on state government devices" for similar reasons. *Ibid.*

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 J.A. 214-221 (House Report 5-12). Most recently, in early 2024, Congress received extensive and detailed classified information and assessments at multiple House committee briefings, a House committee hear-

ing, a briefing for the full House, a briefing for Senate staff, and a Senate committee briefing. See J.A. 711 (Newman Decl. ¶ 122); J.A. 220 (House Report 11).

C. The Act

In April 2024, Congress passed, and the President signed into law, the Protecting Americans from Foreign Adversary Controlled Applications Act (Act), Pub. L. No. 118-50, Div. H, 138 Stat. 955. The Act makes it unlawful for third-party service providers (such as Google or Apple) 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 or providing internet hosting services. § 2(a)(1), 138 Stat. 955-956. The Act does not prohibit continued use of such an application by individuals who have already downloaded it. But as a practical matter, the Act's prohibitions would preclude the application from remaining widely offered to American users. To enforce those prohibition, the Act authorizes the Attorney General to bring suit in district court against third-party service providers for civil penalties and declaratory and injunctive relief. § 2(d), 138 Stat. 957.

The Act provides two pathways for designation of an application as a "foreign adversary controlled application" subject to the Act's prohibitions. First, the Act itself designates any application "operated, directly or indirectly," by "ByteDance"; "TikTok"; or subsidiaries or successors of those companies. § 2(g)(3)(A), 138 Stat. 958-959. Second, the Act provides that a "foreign adversary controlled application" also includes any application that is both (i) operated by a "covered company" that is "controlled by a foreign adversary" (defined by Congress as China, Russia, North Korea, or Iran), and

(ii) "determined by the President to present a significant threat to the national security of the United States" following an administrative process. § 2(g)(1), (3)(B), and (4), 138 Stat. 958-959; see 10 U.S.C. 4872(d)(2). A "covered company" is in turn defined to include a company that, generally speaking, operates an application that permits users to interact with each other and has more than 1 million active monthly users —which would describe many social-media applications like TikTok—but to exclude companies that operate applications "whose primary purpose is to allow users to post product reviews, business reviews, or travel information or reviews." § 2(g)(2), 138 Stat. 958.

The Act's relevant prohibitions take effect 270 days after the designation of an application as foreign-adversary controlled. § 2(a)(2), 138 Stat. 956. For applications owned by ByteDance and TikTok, therefore, the prohibitions take effect on January 19, 2025, 270 days after the Act's enactment on April 24, 2024. *Ibid.*

The Act provides, however, that an application may be removed from the Act's coverage at any time by execution of a "qualified divestiture." § 2(c)(1), 138 Stat. 956-957. A qualified divestiture means a transaction that the President determines (a) will result in the relevant application's "no longer being controlled by a foreign adversary," and (b) "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." § 2(g)(6), 138 Stat. 959. The President also is authorized to grant a single extension, of no more than 90 days, of the prohibition's 270-day effective date if the President certifies to Congress that "a path to executing a qualified divestiture has been identified,"

"evidence of significant progress toward executing" the divestiture "has been produced," and "there are in place the relevant binding legal agreements to enable execution of" the divestiture during the extension period. § 2(a)(3), 138 Stat. 956.

D. Proceedings Below

1. Petitioners are ByteDance, its U.S. subsidiary, and several TikTok users, who filed three petitions for review in the D.C. Circuit challenging the constitutionality of the Act as applied to TikTok. See Act § 3, 138 Stat. 959-960 (providing for exclusive judicial review in the D.C. Circuit). As relevant here, petitioners argued that the Act violates the First Amendment and sought declaratory and injunctive relief.

Petitioners submitted declarations, news articles, and other documents in support of their claims. See ByteDance C.A. Appx. Vols. 1-3; Firebaugh C.A. Appx. Vols. 1-4; ByteDance C.A. Supp. Appx. The government submitted on the public record three redacted declarations by senior intelligence officials and a redacted transcript of a classified hearing before the House Committee on Energy and Commerce. The government also moved to file under seal and *ex parte* the classified, unredacted declarations, a classified version of the hearing transcript, and a classified, unredacted brief for the court of appeals' *in camera* review. See 24-1113 C.A. Doc. 2066895 (July 26, 2024); 24-1113 C.A. Doc. 2069332 (Aug. 9, 2024); 24-1113 C.A. Doc. 2073185 (Sept. 4, 2024). The court granted the motions to file the classified material *ex parte* for *in camera* review, but relied solely on the public record in resolving the petitions. See J.A. 64-65 & n.11.

2. The court of appeals denied the petitions for review. J.A. 1-92.

a. As relevant here, the court of appeals "assume[d] without deciding" that the Act is subject to strict scrutiny, J.A. 24, and held that it "passes muster even under" that "demanding standard," J.A. 25 (citation omitted). The court "emphasize[d]" that its holding was "fact-bound" and grounded in the extensive record recounting the unique national-security risks posed by TikTok. J.A. 32.

At the outset, the court of appeals observed that "both political branches" had engaged in "multi-year efforts" to "investigate the national security risks posed by the TikTok platform" and to determine how best to address those risks. J.A. 32; see J.A. 11-16, 42, 51-52. The court thus noted that the Act "was the culmination of extensive, bipartisan action by the Congress and by successive Presidents." J.A. 32. Against that backdrop, the court concluded that each of the government's two national-security justifications for the Act—preventing China from collecting substantial quantities of U.S. users' data and covertly manipulating content on the platform—was "independently compelling." J.A. 33 (citations omitted).

As to the first interest, the court of appeals observed that China has accumulated extensive datasets on U.S. persons "to support its intelligence and counterintelligence operations," including through "hacking" and by invoking Chinese law to require disclosure to the Chinese government of "data held by Chinese companies." J.A. 34-35. The court further observed that TikTok has more than 170 million U.S. users; that it collects "large swaths of data" on those users, and even on their non-user contacts; and that such data collection is a "significant vulnerability" because the data could be accessed and used by the Chinese government to undermine U.S.

national security, such as through blackmail and espionage. J.A. 38-39.

As to the second interest, the court of appeals explained that the PRC "uses its cyber capabilities to support its influence campaigns around the world" in order to "undermine democracy" and increase the Chinese government's "influence abroad." J.A. 36. The court observed that those efforts include the PRC's "position[ing] itself to manipulate public discourse on TikTok in order to serve its own ends." J.A. 43. Requiring divestiture under these circumstances, the court observed, "follows the Government's well-established practice of placing restrictions on foreign ownership or control where it could have national security implications." J.A. 44. "Were a divestiture to occur," TikTok's "new owners could circulate the same mix of content as before without running afoul of the Act" and "[p]eople in the United States could continue to engage with content on TikTok as at present." *Ibid.* Thus, the court emphasized that the Act does not seek to suppress protected speech or to prevent the expression of pro-China or anti-U.S. views; instead, "the only change worked by the Act is that the PRC could not 'manipulate the public debate through coercion rather than persuasion.'" *Ibid.* (citation omitted).

The court of appeals also rejected petitioners' efforts to dismiss the government's national-security concerns as speculative. The court noted that under well-settled principles, the government's national-security decisions "often must be 'based on informed judgment.'" J.A. 41 (citation omitted). The court explained that here, Congress and the Executive Branch had drawn "reasonable inferences" from the available evidence in concluding that TikTok's continued operations subject to Chinese

control posed serious national-security risks. *Ibid.*; see J.A. 39, 41-42, 47-48.

Next, the court of appeals determined that the Act is narrowly tailored to further Congress's compelling national-security interests because the Act is "limited to foreign adversary control of a substantial medium of communication and include[s] a divestiture exemption." J.A. 48. The court explained that no less-restrictive alternative would have ameliorated the government's national-security concerns. J.A. 48-57. In particular, the court explained that the political Branches had reasonably determined that ByteDance's proposed national security agreement did not provide sufficient government visibility into TikTok's operations or adequate "data protections for Americans," and "still contemplated extensive contacts" between those operating TikTok in the United States and ByteDance's leadership overseas. J.A. 49; see J.A. 50-52 (describing why the proposed national security agreement did not satisfy the government's concerns); J.A. 53-55 (rejecting various other alternative approaches, including disclosure and reporting requirements).

b. Chief Judge Srinivasan concurred in part and in the judgment. J.A. 66-92. He agreed that the Act as applied to TikTok does not violate the First Amendment, but he would have held that the Act is subject to intermediate scrutiny and would not have decided whether the Act would satisfy strict scrutiny. J.A. 66.

Chief Judge Srinivasan reasoned that the Act triggers only intermediate scrutiny because its divestiture requirement is directed to a "designated foreign adversary" based on "reasons lying outside the First Amendment's heartland": the Chinese government's ability "to exploit the TikTok platform" by "harvest[ing] abun-

dant amounts of information about the 170 million" U.S. users and by "covertly manipulat[ing] the content flowing to" those users. J.A. 66, 76. Chief Judge Srinivasan observed that "concerns about the prospect of foreign control over mass communications channels in the United States are of age-old vintage" and "Congress's decision to condition TikTok's continued operation in the United States on severing Chinese control is not a historical outlier." J.A. 67; see J.A. 67-71 (surveying historical examples of legal restrictions on foreign ownership of American communications channels). Chief Judge Srinivasan further reasoned that the Act's "data-protection rationale is plainly content neutral," J.A. 77, and that even if the interest in preventing the PRC's covert manipulation of content on TikTok is "connected to speech," J.A. 78, that rationale does not require strict scrutiny because the Act does not regulate any particular content and instead "only prevents the PRC from secretly manipulating content on a specific channel of communication that it ultimately controls," J.A. 81.

Chief Judge Srinivasan further concluded that the Act satisfies intermediate scrutiny because it advances important government interests without burdening more speech than necessary, for reasons similar to those that the panel majority identified in holding that the Act would survive even strict scrutiny. See J.A. 83-88 (discussing the national-security interests in preventing the Chinese government's data-collection and covert content-manipulation); J.A. 88-91 (concluding that the Act is not substantially broader than necessary to advance those interests).

3. The court of appeals denied petitioners' subsequent motions for injunctions pending certiorari. See 24-1113 C.A. Doc. 2089581 (Dec. 13, 2024). Petitioners

then filed applications in this Court for injunctions pending review. See 24A587 Appl. (ByteDance Appl.); 24A588 Appl. (Firebaugh Appl.). The Court deferred consideration of petitioners' applications, treated the applications as petitions for writs of certiorari, granted the petitions, and ordered the parties to file simultaneous briefs.

SUMMARY OF ARGUMENT

The Act is entirely consistent with the First Amendment. It addresses the serious threats to national security posed by the Chinese government's control of TikTok, a platform that harvests sensitive data about tens of millions of Americans and would be a potent tool for covert influence operations by a foreign adversary. And the Act mitigates those threats not by imposing any restriction on speech, but instead by prohibiting a foreign adversary from controlling the platform. That targeted, content-neutral divestiture requirement complies with the First Amendment under any potentially applicable standard of review.

A. As a threshold matter, the Act's prohibition on foreign-adversary ownership and control does not implicate the First Amendment rights of any petitioner. ByteDance is a foreign entity operating abroad and thus lacks First Amendment rights. Nor can it manufacture a First Amendment right by laundering its overseas activities through its American subsidiary, which has no First Amendment right to be controlled by a foreign adversary. And TikTok users likewise have no First Amendment right to post content on a platform controlled by a foreign adversary.

B. Even if the First Amendment were implicated, the Act would be subject only to intermediate scrutiny because it is a content-neutral regulation of conduct

that only incidentally affects protected speech. The Act does not target or regulate speech; instead, it restricts the provision of services to a platform that Congress determined was controlled by a foreign adversary. The Act is facially content-neutral, and neither of the national-security interests justifying the Act is content-based. The interest in preventing a foreign adversary from harvesting Americans' sensitive data does not involve speech at all. And the interest in preventing covert content manipulation by a foreign adversary seeks to prevent all such manipulation regardless of the content or viewpoint being advanced.

C. In any event, the Act would survive any level of First Amendment scrutiny because it is narrowly tailored to further the compelling national-security interests in preventing mass data collection and covert content-manipulation by a foreign adversary.

1. The government has a compelling interest in preventing the PRC from harvesting vast quantities of Americans' sensitive data. That is particularly so given the PRC's history of collecting such data and engaging in cyber attacks against Americans, as well as laws that give the PRC full (and secret) access to data held by Chinese companies and their subsidiaries. The Act is narrowly tailored to serve that compelling interest. It surgically addresses the risk by requiring only that TikTok be divested from a company subject to PRC control, which could leave all protected expression on the platform unchanged. And petitioners' proposed alternative of installing a third-party company as a monitor would not address the government's national-security concerns because effective monitoring would be impossible.

This Court could uphold the Act based solely on the government's compelling interest in preventing mass data collection by a foreign adversary. Contrary to petitioners' assertion, the government is not required to show that Congress would have adopted the Act had it been concerned about data collection alone, and not also covert manipulation. A statute that is narrowly tailored to serve a compelling interest can be sustained on that basis even if Congress also sought to further other interests that may not satisfy strict scrutiny.

2. In any event, the government also has a compelling interest in preventing covert manipulation of the TikTok platform by the PRC, which could engage in such malign influence operations using TikTok to undermine the United States. That interest is particularly compelling because the PRC has engaged in other forms of covert influence operations using social-media platforms in the past and because ByteDance in particular has engaged in covert content manipulation in other countries, including at the behest of the PRC.

The Act is the least restrictive means of furthering the government's compelling interest. To preclude the PRC from covertly manipulating the platform, the Act requires only divestiture of TikTok. The Act fits comfortably within a long tradition of regulation of foreign ownership of domestic channels of communication and other critical infrastructure. And petitioners' proposed alternatives of disclosure and monitoring would not address the government's concerns. By definition, disclosure is not an effective remedy for *covert* influence operations, and a third-party monitor could not feasibly prevent manipulation.

3. Petitioners' remaining arguments lack merit. This Court has upheld far more direct restrictions on

speech under strict scrutiny, such as a ban on certain communications to foreign terrorist organizations and a ban on solicitation of campaign funds by judicial candidates. And the Act's exclusion (under the presidential-designation pathway) for applications with the primary purpose of facilitating business, product, and travel reviews shows that Congress was cognizant of constitutional concerns and limited the Act's reach to the applications directly posing known national-security threats.

4. Although the court of appeals relied only on the public record in upholding the Act, the classified record describes the threat landscape in more detail and thus provides further support for the statute's constitutionality.

ARGUMENT

The Act is consistent with the First Amendment because petitioners have not identified a burden on any cognizable First Amendment rights and, even if they had, the Act at most incidentally burdens protected speech. In any event, the Act is narrowly tailored to further the compelling interests in preventing the threats to national security posed by foreign-adversary control of TikTok: namely, the collection of sensitive data of U.S. persons and malign foreign influence of the platform targeting U.S. persons. The Act therefore satisfies any level of First Amendment scrutiny.

A. The Act Does Not Trigger First Amendment Scrutiny

1. The Act does not implicate the First Amendment because it does not burden any First Amendment rights of ByteDance, its U.S. subsidiary, or TikTok's users.

a. ByteDance is a "foreign organization[] operating abroad" and thus "ha[s] no First Amendment rights" to begin with. *Agency for International Development* v. *Alliance for Open Society International, Inc.*, 591 U.S.

430, 436 (2020) (*AOSI*). Accordingly, even though application of the proprietary recommendation algorithm and content-moderation policies on the TikTok platform are a form of speech, see *Moody* v. *NetChoice, LLC*, 603 U.S. 707, 728 (2024), ByteDance itself has no cognizable First Amendment claim with respect to any alleged abridgement of that speech, including the required severing of its ties with its U.S. subsidiary and the TikTok platform. See J.A. 72-74.

b. Nor does ByteDance's U.S. subsidiary have any such claim. The Act targets only content manipulation associated with overseas application of the proprietary foreign algorithm and recommendation engine, which are controlled by ByteDance. ByteDance also has ultimate control over the U.S. subsidiary, which has no authority or technical ability to alter the algorithm or recommendation engine, and instead must simply follow ByteDance's directives (and thus ultimately any directives from the PRC) with respect to applying the algorithm and engine to (covertly) manipulate content on TikTok in the United States. As a result, even though such manipulation might appear on the surface to be the act of the U.S. subsidiary, in reality the subsidiary is not speaking for itself; it is simply serving as a compelled mouthpiece for ByteDance's speech, which is not entitled to First Amendment protection. *AOSI*, 591 U.S. at 436. The U.S. subsidiary has no First Amendment right to be controlled by a foreign adversary; nor does it have a First Amendment right to use an algorithm developed, maintained, and controlled by a foreign adversary, and which Congress has determined poses a national-security risk. Cf. *NetChoice*, 603 U.S. at 747 (Barrett, J., concurring) (observing that "a social-media platform's foreign ownership and control over its

content-moderation decisions might affect whether laws overriding those decisions trigger First Amendment scrutiny"). Just as Americans "cannot export their own First Amendment rights" to foreigners abroad, *AOSI*, 591 U.S. at 438, a foreign adversary abroad cannot manufacture First Amendment rights for itself by the simple expedient of using an American puppet as a mouthpiece.

Although petitioners have asserted (ByteDance Appl. 19) that the U.S. subsidiary engages in some content-moderation or other speech of its own *after* application of the foreign algorithm and engine, the Act does not target that speech; to the contrary, the Act would "leave untouched [the subsidiary's] expression on a post-divestment version of the" TikTok platform, including such "speech and curation choices." J.A. 74. Indeed, the Act even permits the operator of a post-divestiture TikTok to use a "recommendation engine" with "the same algorithm," which further underscores that the Act targets only the control of that algorithm and the TikTok platform by a foreign adversary, not the protected speech of any U.S. person. J.A. 75. For similar reasons, the Act does not impose a "disproportionate burden" (J.A. 26) on petitioners' expressive activity: The Act imposes burdens only on unprotected activity overseas and if ByteDance ultimately refuses to divest TikTok, any resulting burden on petitioners' protected speech would be attributable to ByteDance.

c. As for the claims of TikTok users, nothing in the Act regulates their speech. Congress addressed national-security concerns posed by the ownership and control of TikTok by a foreign adversary (which lacks First Amendment rights), and specifically by that adversary's ability to engage in mass data collection and cov-

ert content manipulation. The Act accordingly regulates service providers that support TikTok and other similar applications. See § 2(a)(1), 138 Stat. 955-956. The Act does not regulate the speech (or even the conduct) of any of the TikTok-user petitioners. Those petitioners remain free under the Act to say whatever they would like, including on numerous other social-media platforms and on a post-divestiture TikTok itself.

To be sure, ByteDance's failure to divest TikTok by the congressionally mandated deadline might incidentally affect the reach of petitioners' speech by resulting in the impairment or disabling of the TikTok platform in the United States. But that consequence would properly be attributable to ByteDance's refusal to divest or to allow TikTok's independent use of the algorithm in the United States—and instead to insist that the algorithm remain controlled by a foreign adversary. Petitioners do not have a constitutional right to speak on a TikTok platform that is controlled by a foreign adversary. Cf. *Heffron* v. *International Society for Krishna Consciousness, Inc.*, 452 U.S. 640, 647 (1981) ("[T]he First Amendment does not guarantee the right to communicate one's views at all times and places or in any manner that may be desired.").

2. This case is thus akin to *Arcara* v. *Cloud Books, Inc.*, 478 U.S. 697 (1986), which held that "the First Amendment is not implicated" by the forced closure of a bookstore as a public-health nuisance, even though the store indisputably facilitated protected speech. *Id.* at 707. The Court explained that a restriction that does not target speech is subject to First Amendment scrutiny "only where it was conduct with a significant expressive element that drew the legal remedy in the first place, * * * or where a statute based on a nonexpres-

sive activity has the inevitable effect of singling out those engaged in expressive activity." *Id.* at 706-707 (footnote omitted). The Court concluded that although the store's owners would have to "move their bookselling business to another location" as a result of the closure, that did not burden speech in a way that triggered First Amendment scrutiny. *Id.* at 706.

Like the public-health law in *Arcara*, the Act here does not target protected speech as such. Instead, the Act targets the control of TikTok by a foreign adversary because of serious national-security concerns, and the Act would permit all protected speech on the platform to continue unabated on a post-divestiture TikTok. Petitioners' protected expressive conduct did not elicit the Act's remedies in the first place; nor does the Act single out petitioners because of their protected expressive activity on TikTok. That petitioners might have "to move their [social-media posts] to another location" if ByteDance elects not to divest TikTok does not implicate the First Amendment in these circumstances. *Arcara*, 478 U.S. at 706; see J.A. 77; cf. *Virginia* v. *Hicks*, 539 U.S. 113, 123 (2003) (statute forbidding person with prior civil violations from entering otherwise public forum "no more implicates 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").

B. Even If Petitioners Had Raised Cognizable First Amendment Claims, The Act At Most Triggers Intermediate Scrutiny

Even if the Act required more exacting First Amendment review, it would warrant only intermediate scrutiny. This Court has long recognized that content-

neutral regulations of conduct that impose only "incidental" burdens on protected expression trigger at most intermediate scrutiny. *Rumsfeld* v. *Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 62 (2006). And here, the Act's effect on protected speech is only incidental, and it does not impose any content-based restrictions. See J.A. 77-82.

1. As noted, Congress adopted the Act to protect Americans from vast data collection and covert content-manipulation. See pp. 2-6, *supra*; pp. 29-31, *infra*. The "data-protection rationale has nothing to do with the expressive activity taking place on the TikTok platform." J.A. 77. And the covert-content-manipulation justification, while nominally relating to speech, does not aim at *constitutionally protected* speech because it targets only the covert manipulation of content by a foreign adversary that lacks First Amendment rights. As a result, any burden that the Act might impose on the constitutionally protected speech of user petitioners (if ByteDance opts not to divest) or of ByteDance's U.S. subsidiary (to the extent it engages in its own protected speech) would be purely incidental.

This Court's precedents illustrate the point. In *United States* v. *O'Brien*, 391 U.S. 367 (1968), for example, the Court held that a statute prohibiting the destruction or mutilation of a military draft card imposed only an incidental burden on speech because "there is nothing necessarily expressive about such conduct," even though the defendant had burned his draft card as a form of political protest. *Id.* at 375. In *Ward* v. *Rock Against Racism*, 491 U.S. 781 (1989), the Court held that a city guideline prohibiting the use of sound trucks imposed only an incidental burden on speech because the purpose of the guideline was "to control noise lev-

els" and "retain the character of [the recreation area] and its more sedate" nature. *Id.* at 792. And in *Turner Broadcasting System, Inc.* v. *FCC*, 512 U.S. 622 (1994) (*Turner I*), the Court held that a statute requiring cable television systems to carry certain local television stations imposed only an incidental burden on speech because it was "meant to protect broadcast television" from "unfair competition by cable systems." *Id.* at 652.

Here, too, there is nothing necessarily expressive about choosing to post on a social-media platform *controlled by a foreign adversary* in particular, as opposed to one not controlled by such an entity. And the prohibition on ownership or control of TikTok by a foreign adversary does not regulate the content or viewpoints expressed on the platform, but instead addresses only the national-security risks that flow from that ownership or control. See *Sorrell* v. *IMS Health Inc.*, 564 U.S. 552, 567 (2011) (explaining that "the First Amendment does not prevent restrictions directed at commerce * * * from imposing incidental burdens on speech").

Nor does the Act impose any content-based restriction on speech. See J.A. 78-82. A content-based restriction is one that "discriminate[s] based on 'the topic discussed or the idea or message expressed.'" *City of Austin* v. *Reagan National Advertising of Austin, LLC*, 596 U.S. 61, 73-74 (2022) (quoting *Reed* v. *Town of Gilbert*, 576 U.S. 155, 171 (2015)). Nothing in the text or operation of the Act discriminates based on content. Nor are the national-security interests underlying the Act content-based: The data-collection interest does not concern content at all, and the covert-content-manipulation interest seeks to "prevent the PRC's secret curation of content flowing to U.S. users *regardless* of the topic, idea, or message conveyed." J.A. 79.

Petitioners thus badly miss the mark in arguing that Congress's true motive was to suppress particular content or viewpoints prevalent on TikTok. As Chief Judge Srinivasan observed, "the concern is with the PRC's manipulation of the app to advance China's *interests*—not China's views," and thus would apply equally to PRC efforts "to augment *anti*-China, *pro*-U.S. content" on TikTok, such as "to stir an impression of elevated anti-China sentiment" in order "to conjure a justification for actions China would like to take against the United States." J.A. 80. At most, therefore, the Act reflects a "speaker (non)preference" that "is not grounded in a content preference." J.A. 81. And nothing in the First Amendment prohibits targeting a foreign entity operating abroad that is subject to the control of a foreign adversary.

2. Moreover, the Act does not affect the ability of petitioners to speak in the United States using methods *other than* posting on a platform subject to the PRC's control; indeed, nothing in the Act precludes petitioners from posting whatever they like on a post-divestiture TikTok itself. So at most the Act's restriction on foreign-adversary control might be analogized to "a time, place, or manner regulation," which also is "generally subject to intermediate scrutiny." J.A. 81 (citing *Clark* v. *Community for Creative Non-Violence*, 468 U.S. 288 (1984), and *Ward*, *supra*). In particular, a content-neutral time, place, or manner restriction on otherwise-protected speech does not violate the First Amendment where "ample alternative modes of communication" are feasible. *Members of City Council* v. *Taxpayers for Vincent*, 466 U.S. 789, 812 (1984). Here, multiple alternative social-media platforms exist for communication; that some petitioners might believe that "more people may

be more easily and cheaply reached by [TikTok]" for their particular posts than by other platforms "is not enough to call forth constitutional protection" in light of the serious national-security concerns identified by the Legislative and Executive Branches. *Kovacs* v. *Cooper*, 336 U.S. 77, 88-89 (1949).

Even with respect to the availability of TikTok itself, moreover, petitioners overstate the Act's likely effect on TikTok's users. Notwithstanding petitioners' alarmist predictions, this Court should not presume that, if it were to sustain the Act's application to TikTok, ByteDance would actually choose to permanently shut down TikTok in the United States—and entirely squander that platform domestically—rather than effectuate a qualified divestiture that would recoup substantial value. At a minimum, Congress could reasonably have anticipated that the Act would result in such a divestiture. Cf. J.A. 64 (observing that TikTok "has assets that can be sold apart from the recommendation engine, including its codebase; large user base, brand value, and goodwill; and property owned by TikTok").

The assessment of petitioners' First Amendment claims should take account of that practical reality. Cf. *Trump* v. *Mazars USA, LLP*, 591 U.S. 848, 867 (2020) (courts should not be "'blind'" to "what 'all others can see and understand'") (brackets and citation omitted); *United States* v. *Stanchich*, 550 F.2d 1294, 1300 (2d Cir. 1977) (Friendly, J.) ("Judges are not required to exhibit a naivete from which ordinary citizens are free."). If ByteDance effects a qualified divestiture, TikTok's users can continue to post whatever they desire on the post-divestiture platform, and the successor company operating TikTok in the United States (perhaps even the same company that is now ByteDance's U.S. subsid-

iary, made newly independent) can moderate and curate content in any manner it chooses. Even ByteDance and the PRC could post on TikTok; they just could not covertly manipulate the content on the platform (which, as foreign entities operating abroad, they have no First Amendment right to do anyway). And if ByteDance opts not to make a qualified divestiture (perhaps because of restrictions imposed by the PRC), the resulting unavailability of TikTok in the United States would properly be attributable to ByteDance's and the PRC's choice not to relinquish their control over TikTok or use of the algorithm.

C. In Any Event, The Act Is Narrowly Tailored To Further Compelling National-Security Interests

At all events, the court of appeals correctly determined that the Act would satisfy any level of scrutiny. Intermediate scrutiny requires a showing that the Act "advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests." *Turner Broadcasting System, Inc.* v. *FCC*, 520 U.S. 180, 189 (1997) (*Turner II*) (citing *O'Brien*, 391 U.S. at 377). Strict scrutiny requires a showing that the Act is "narrowly tailored to serve a compelling interest." *Williams-Yulee* v. *Florida Bar*, 575 U.S. 433, 444 (2015). The Act satisfies either standard because it is narrowly tailored to further the compelling national-security interests in preventing mass data harvesting and covert content manipulation on the TikTok platform by a foreign adversary.

1. The Act is narrowly tailored to further the compelling national-security interest in preventing mass harvesting of Americans' data by a foreign adversary

a. Petitioners do not seriously contest that the government has a compelling interest in preventing the widespread collection of Americans' data by the PRC. Nor could they: the Executive and Legislative Branches have determined that the "PRC is the most active and persistent cyber espionage threat to U.S. government, private-sector, and critical infrastructure networks." J.A. 34. The PRC "has engaged in 'extensive and yearslong efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations.'" *Ibid.* Those efforts include "hacking operations," such as breaching the systems of the United States Office of Personnel Management "and taking 'reams' of personal data, stealing financial data on 147 million Americans from a credit-reporting agency, and 'almost certainly' extracting health data on nearly 80 million Americans from a health insurance provider." *Ibid.* The PRC has additionally focused on "using 'its relationships with Chinese companies,' making 'strategic investments in foreign companies,' and 'purchasing large data sets,'" such as its attempt "'to acquire sensitive health and genomic data on U.S. persons' by investing in firms that have or have access to such data." J.A. 34-35.

The PRC is well positioned to deploy potent "hybrid commercial threat[s]" because of laws "that enable it to access and use data held by Chinese companies." J.A. 35; see J.A. 673-676 (Newman Decl. ¶¶ 16-25) (describing various laws). "U.S. subsidiaries of Chinese parent corporations remain subject to PRC jurisdiction and laws," and "the PRC can access information from and

about U.S. subsidiaries and compel their cooperation with PRC directives." J.A. 657-658 (Vorndran Decl. ¶ 10). As a result, the PRC can "conduct espionage, technology transfer, data collection, and other disruptive activities under the disguise of an otherwise legitimate commercial activity." J.A. 35. And as "'part of the PRC's broader geopolitical and long-term strategy to undermine U.S. national security,'" "the PRC endeavors strategically to pre-position commercial entities in the United States that the PRC can later 'co-opt'" in the manner described above. *Ibid.*

The political Branches thus reasonably concluded that the "ByteDance and TikTok entities 'would try to comply if the PRC asked for specific actions to be taken'" on the TikTok platform in the United States. J.A. 36; see J.A. 673 (Newman Decl. ¶ 17) ("Because of the authoritarian structures and laws of the PRC regime, Chinese companies lack meaningful independence from the PRC's agenda and objectives."). "ByteDance, which is subject to PRC laws requiring cooperation with the PRC, could do so by acting unilaterally or by conscripting its U.S. entities." J.A. 36. And "PRC-based companies like ByteDance are compelled to cooperate with PRC law enforcement requests and are prohibited from disclosing that cooperation." J.A. 687 (Newman Decl. ¶ 78(a)); see J.A. 647 (Blackburn Decl. ¶ 71).

The combination of the PRC's deep interest in data collection and its ability to control and coopt Chinese-based companies like ByteDance is particularly concerning in light of the nature and sheer amount of data that TikTok collects. "TikTok automatically collects large swaths of data about its users, including device information (IP address, keystroke patterns, activity

across devices, browsing and search history, etc.) and location data (triangulating SIM card or IP address data for newer versions of TikTok and GPS information for older versions)." J.A. 38. "It may also collect image and audio information (including biometric identifiers and biometric information such as faceprints and voiceprints); metadata (describing how, when, where, and by whom content was created, collected, or modified); and usage information (including content that users upload to TikTok)." *Ibid.* "Access to such information could, for example, allow the PRC to 'track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.'" J.A. 39 (quoting 85 Fed. Reg. at 48,637). That risk is not hypothetical: "Forbes reported that ByteDance employees used IP address locations to track multiple journalists covering the company." J.A. 661 (Vorndran Decl. ¶ 29); see J.A. 697 (Newman Decl. ¶ 98); J.A. 217 (House Report 8).

As the court of appeals observed, petitioners "do[] not deny that [TikTok] collects a substantial amount of data on its users," and instead merely quibble with details in a manner that "misses the forest for the trees." J.A. 38-39. For example, petitioners have disputed the finding "that TikTok collects 'precise' location information from users." ByteDance Appl. 15. But in the lower court, petitioners represented only that "*current versions* of the application do not collect *GPS* location information." 24-1113 C.A. Doc. 2068242, at 22-23 (Aug. 5, 2024) (emphases added). Petitioners conspicuously declined to deny that TikTok currently collects other location data (by using, say, IP addresses rather than GPS); that prior versions of TikTok did collect GPS data; or that the location data was precise enough that

ByteDance was able to track journalists even without using GPS data. Nor did petitioners represent that TikTok would never change its policies and collect GPS data once again. In any event, none of petitioners' factual quibbles undermines the fundamental point that the Executive and Legislative Branches were understandably concerned about the PRC's access to location data—and the vast quantity of other data—that TikTok collects and reasonably acted to address those concerns. See J.A. 39 (observing that "TikTok's own declarants provide support for the Government concern" about data collection).

Petitioners have argued that the "data-protection interest is so underinclusive that it 'raises serious doubts about whether the government is in fact pursuing the interest it invokes, rather than disfavoring a particular speaker or viewpoint.'" ByteDance Appl. 28 (quoting *Brown* v. *Entertainment Merchants Association*, 564 U.S. 786, 802 (2011)); see Firebaugh Appl. 31. But the Executive and Legislative Branches identified TikTok —and the massive scale of sensitive data that it collects —as a uniquely severe threat, especially in light of past instances of data collection, ByteDance's corporate structure, and the PRC's hybrid-commercial-threat strategy. See pp. 2-6, 29-31, *supra*. Although petitioners assert (ByteDance Appl. 28-29) that other Chinese-based applications collect comparable types of data from their users, petitioners do not contend that such applications have anywhere near the reach of TikTok's 170 million monthly users or the same track record of taking action at the behest of the PRC. See J.A. 42. Congress reasonably could have viewed those differences as sufficiently reducing the national-security risks to avoid requiring immediate divestiture of those

applications (while leaving open the possibility of requiring divestiture in the future under the presidential-designation pathway, should circumstances evolve).

In that respect, had the Act addressed *only* TikTok, it still would not have been fatally underinclusive; after all, "the First Amendment imposes no freestanding 'underinclusiveness limitation,'" and government policymakers "need not address all aspects of a problem in one fell swoop" but instead "may focus on their most pressing concerns." *Williams-Yulee*, 575 U.S. at 449 (citation omitted); see J.A. 42. And the fact that Congress chose to give the President authority under the Act to designate certain other entities that raise similar risks further mitigates any perceived underinclusiveness concern.

b. The Act is narrowly tailored to address the government's compelling interest in protecting against the PRC's access to and control over TikTok's data-collection activities. Indeed, the Act adopts arguably the narrowest solution of all: It simply seeks to eliminate Chinese control over TikTok, so that whichever company distributes and runs the platform in the United States post-divestiture will not be beholden to demands from the PRC or a Chinese-controlled parent company to hand over the data of American users. The targeted solution of divestiture is therefore precisely aimed at minimizing the chances that the data could wind up in the hands of a foreign adversary.

The supposedly less-restrictive alternatives identified by petitioners would not address the government's concerns. ByteDance's proposed "national security agreement" (see ByteDance Appl. 31) had numerous shortcomings: among other things, it "still permitted certain data of U.S. users to flow to China"; "still per-

mitted ByteDance executives to exert leadership control and direction over TikTok's US operations"; and "would ultimately have relied on the Executive Branch trusting ByteDance to make day-to-day business decisions that enforce the mitigation measures even as the Executive Branch lacked the resources and capabilities to fully monitor and verify ByteDance's compliance." J.A. 686 (Newman Decl. ¶ 75). And the "ring-fenced storage of U.S. data in the Oracle cloud" (ByteDance Appl. 31) is a mirage: ByteDance "would never agree" to "cease collecting U.S. user data or sending it to Beijing to train the algorithm" that drives TikTok, J.A. 705-706 (Newman Decl. ¶ 115(a)(iv)), and in any event neither Oracle nor any other third party would be able to comprehensively review and verify compliance as a practical matter, J.A. 691-692 (Newman Decl. ¶ 85(a)-(c)).

In short, the "Executive Branch concluded that ByteDance lacked the baseline trust required of parties to mitigation agreements." J.A. 694 (Newman Decl. ¶ 91); see J.A. 15 ("The Executive also did not trust that ByteDance and [one of its subsidiaries] would comply in good faith with the [proposed national security agreement]."). That lack of trust that ByteDance could or would comply in good faith is also why simply extending legal prohibitions on the export of certain data to ByteDance (see ByteDance Appl. 30-31) would not have addressed the government's national-security concerns.

Petitioners have also suggested (Firebaugh Appl. 32) that disclosure would have solved the data-collection concern. That suggestion misapprehends the concern, which is that the PRC could compel ByteDance and its subsidiaries to give it vast amounts of user data, and that the PRC would use that information (aggregated

with other data, including information obtained through data breaches and cyber espionage) as part of its intelligence activities and efforts to undermine the United States' national security. See J.A. 34-42. Disclosure would not address that concern at all.

c. Because the Act is narrowly tailored to further the compelling national-security interest in preventing the PRC from harvesting Americans' sensitive data, this Court can affirm the judgments below on that basis alone. Although Chief Judge Srinivasan stated that the government had not argued below that the Act could be sustained by relying only on that basis, see J.A. 78, nothing required the government to specifically make that further point after establishing that preventing mass data collection was a proper basis for the Act. In any event, the government obviously preserved the claim that the Act does not violate the First Amendment—and "[o]nce a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise arguments they made below," *Yee* v. *City of Escondido*, 503 U.S. 519, 534 (1992). This Court should not invalidate an Act of Congress where, as here, the statute has a valid constitutional basis.

Citing *Mt. Healthy City Board of Education* v. *Doyle*, 429 U.S. 274 (1977), and *Village of Arlington Heights* v. *Metropolitan Housing Development Corp.*, 429 U.S. 252 (1977), petitioners have asserted that the Act may not be upheld on the data-collection rationale unless the government can demonstrate "that Congress would have passed the Act for data-protection reasons alone." ByteDance Appl. 28; see Firebaugh Appl. 31. That is doubly wrong.

First, the sort of counterfactual analysis prescribed by *Mt. Healthy* may be appropriate when evaluating "discrete governmental decision[s]," *Texas* v. *Lesage*, 528 U.S. 18, 21 (1999) (per curiam), such as the nonrenewal of the employee contract in *Mt. Healthy* or the zoning decision in *Arlington Heights*. But petitioners have not identified any instance in which this Court has applied *Mt. Healthy* to ferret out a supposedly "improper motive" (ByteDance Appl. 28) in a First Amendment challenge to an Act of Congress, or otherwise required the government to produce evidence of what Congress would have enacted in a counterfactual world. Such requirements would contravene the settled principle that "this Court will not strike down an otherwise constitutional statute on the basis of an alleged illicit legislative motive." *O'Brien*, 391 U.S. at 383; see *Barenblatt* v. *United States*, 360 U.S. 109, 132 (1959) ("So long as Congress acts in pursuance of its constitutional power, the Judiciary lacks authority to intervene on the basis of the motives which spurred the exercise of that power."); cf. *Sable Communications of California, Inc.* v. *FCC*, 492 U.S. 115, 133 (1989) (Scalia, J., concurring) ("Neither due process nor the First Amendment requires legislation to be supported by committee reports, floor debates, or even consideration, but only by a vote").

Second, and in any event, the counterfactual analysis that petitioners demand applies only when a government action is taken in part for an *unconstitutional* reason, such as retaliating against protected speech, see *Mt. Healthy*, 429 U.S. at 287, or racial discrimination, see *Arlington Heights*, 429 U.S. at 252, 270 n.21. Here, however, the other interest that Congress sought to further—preventing covert manipulation by a foreign

adversary—is not constitutionally prohibited; instead, petitioners assert that it is not sufficient to satisfy strict scrutiny because Congress's chosen method sweeps in protected speech. But even if that were correct, it would provide no basis for invalidating the Act: A statute that is narrowly tailored to serve a compelling interest can be sustained on that basis even if (as often may be the case) Congress also sought to further other interests that may not themselves satisfy strict scrutiny.

2. The Act is narrowly tailored to further the compelling national-security interest in preventing covert manipulation of content by a foreign adversary

a. The Act addresses another compelling national-security concern: the covert manipulation of content on an important medium of communication by a foreign adversary. As intelligence officials explained, that kind of malign foreign influence and algorithmic manipulation could be used to advance Chinese geopolitical interests, such as by launching "campaign[s] of harassment against pro-democracy dissidents in the United States" (as "dozens of PRC officials" have already been indicted for doing) or by "magnify[ing] U.S. societal divisions in ways favorable to the PRC." J.A. 633-634 (Blackburn Decl. ¶¶ 28-29); see J.A. 661-662 (Vorndran Decl. ¶¶ 30-33). Indeed, ByteDance has already "taken action in response to PRC demands to censor content *outside* of China" and "ha[s] a demonstrated history of manipulating the content on [its] platforms, including at the direction of the PRC." J.A. 641, 644 (Blackburn Decl. ¶¶ 54, 58).

In their applications for emergency relief, petitioners raised a factbound objection to the court of appeals' crediting those representations on the ground that petitioners did not "'squarely den[y]'" them; according to

petitioners, they could not deny the statements because they were "vague" and "*all* the supporting detail was submitted *ex parte*." ByteDance Appl. 34 (citation omitted). But there is nothing vague about a representation that ByteDance has engaged in censorship or manipulated content on its platforms *at the direction of the PRC*. ByteDance does not explain why it needs to see the government's classified evidence to be able to deny that it has done that. In any event, in this "sensitive and weighty" context of "national security and foreign affairs," the "evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference." *Holder* v. *Humanitarian Law Project*, 561 U.S. 1, 33-34 (2010).

Petitioners have mischaracterized the concern about content manipulation as involving a desire to censor particular content or viewpoints on TikTok. See, *e.g.*, ByteDance Appl. 24 (asserting that Congress "had the broader, illegitimate interest in *itself altering the content* on TikTok" and "'[c]orrecting the mix of speech'" on the platform) (brackets and citation omitted); Firebaugh Appl. 18 (asserting that the Act attempts to "ban[] speech of Americans because of concerns that foreign governments might benefit from it or add their own voice to it"). As noted, nothing in the Act prevents exactly the same mix of content and viewpoints from being expressed on a post-divestiture TikTok. See J.A. 44. The national-security concerns stem from the PRC's ability to covertly manipulate the recommendation algorithm in order to further its own interests. That has nothing to do with hostility to particular content or viewpoints as such; such manipulation could just as easily involve promoting anti-China rather than pro-China views, or concern any topic that the PRC decides would

further its strategic interests to manipulate. See p. 26, *supra*.

Indeed, the Act echoes approaches previously taken by Congress and the Executive Branch to address the national-security risks arising from foreign-owned commercial entities. See J.A. 44, 67-70. Congress has long regulated foreign ownership of, or control over, companies operating in particular industries. See, *e.g.*, *Moving Phones Partnership* 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), cert. denied, 511 U.S. 1004 (1994); 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). The FCC has recently denied or revoked licenses to operate communications lines in the United States under 47 U.S.C. 214 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, 1162-1163 (D.C. Cir. 2023). And Congress has broadly regulated foreign investment in the United States on the basis of national security, including by authorizing the President to suspend or prohibit foreign investment transactions that threaten to impair national security. See 50 U.S.C. 4565 (Committee on Foreign Investment in the United States). As Chief Judge Srinivasan observed, the Act's focus on "severing Chinese control is not a historical outlier," but instead "is in line with a historical pattern." J.A. 67.

Petitioners have attempted (*e.g.*, Firebaugh Appl. 24-25) to distinguish the limitations on the ownership of radio stations on the ground that they involve the scarce resource of the broadcast spectrum, but that prohibition extends even to indirect foreign control and rests on national-security grounds as well. J.A. 68, 70. That TikTok reaches 170 million Americans per month and has become one of the most prominent methods of communication about everything from "core political speech" to "more lighthearted fare" (Firebaugh Appl. 12) only exacerbates, not mitigates, the national-security concerns. The First Amendment would not have required our Nation to tolerate Soviet ownership and control of American radio stations (or other channels of communication and critical infrastructure) during the Cold War, and it likewise does not require us to tolerate ownership and control of TikTok by a foreign adversary today. As the author of the First Amendment observed, "[s]ecurity against foreign danger is * * * an avowed and essential object of the American Union." *The Federalist No. 41*, at 269 (Madison) (Jacob E. Cooke ed. 1961).

b. The Act is narrowly tailored to further the government's compelling interest in preventing the PRC from covertly manipulating the recommendation algorithm and content to further its own interests and harm the United States. As with the data-collection concern, the Act implements arguably the narrowest possible remedy: removing Chinese control over TikTok to prevent such manipulation by the PRC.

Petitioners again suggest (ByteDance Appl. 26-27; Firebaugh Appl. 30) that requiring disclosure of the manipulation would be less restrictive. But disclosure does not solve the problem of *covert* manipulation by a foreign adversary like the PRC. See J.A. 54 (calling such

a solution "naïve"). As petitioners appear to recognize, ByteDance obviously could not be expected to comply with a directive to notify the government and the public if it were being used in a covert influence operation by the PRC. And Congress and the Executive Branch could reasonably determine that petitioners' proposed alternative—an anemic standing disclosure that the PRC *could*, at some unspecified point, engage in manipulation—would be useless. See J.A. 687-689 (Newman Decl. ¶¶ 78-80). Nor could manipulation of TikTok's dynamic recommendation algorithm or the constantly changing content on the platform be effectively detected or monitored by Oracle, even if it were given access to the voluminous and ever-changing source code (which is 20 times larger than the code for the entire Windows operating system). See *ibid.*; see also J.A. 384 (TikTok deploys software updates "approximately 1,000" times "each day") (citation omitted).

Those same considerations preclude ByteDance's proposed "national security agreement" from being a viable alternative. See J.A. 49-53. That proposal would have required the government to continually monitor compliance with the agreement—a result that not only would be impracticable, but also would "[e]ntangl[e] the U.S. government in the daily operations of a major communications platform" and thereby "raise its own set of First Amendment questions." J.A. 53; see J.A. 15 (explaining that the Executive Branch does not "have 'sufficient visibility into and resources to monitor' compliance") (brackets omitted). Given the lack of trust in the good-faith compliance of ByteDance and the PRC, divestiture of TikTok from Chinese control was the only effective means of addressing Congress's national-security concerns.

3. Petitioners' remaining arguments lack merit

a. Petitioners have erred in asserting (*e.g.*, ByteDance Appl. 3) that the court of appeals improperly watered down the strict-scrutiny standard in rejecting their challenge to the Act. This Court has upheld even direct abridgements of speech under strict scrutiny, and the lower court's decision fits comfortably within the principles reflected in those precedents. For example, in *Humanitarian Law Project*, *supra*, the Court affirmed a prohibition on communications imparting a "specific skill" or "specialized knowledge" to foreign terrorist organizations. 561 U.S. at 27 (citation omitted). The Court explained that where national security and foreign policy are concerned, "[i]t is vital * * * 'not to substitute [the Court's] own evaluation of evidence for a reasonable evaluation by the Legislative Branch,'" especially when Congress has attempted to "confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess." *Id.* at 34 (citation and ellipsis omitted); cf. *Hernandez* v. *Mesa*, 589 U.S. 93, 113 (2020) ("Foreign policy and national security decisions are 'delicate, complex, and involve large elements of prophecy' for which 'the Judiciary has neither aptitude, facilities, nor responsibility.'") (brackets and citation omitted). That equally describes this case: the political Branches have determined based on years of careful study that Chinese control of TikTok presents a national-security threat that the PRC could unleash at a time of its choosing, and that divesting TikTok from Chinese control would help to neutralize that threat. Petitioners provide no sound basis for this Court to second-guess that judgment.

Similarly, in *Williams-Yulee*, *supra*, the Court upheld a ban on personal solicitation of campaign funds by judicial candidates on the ground that the State had a compelling interest in "'protecting the integrity of the judiciary,'" and the ban was narrowly tailored to further that interest because it was "aim[ed] squarely at the conduct most likely to undermine public confidence in the integrity of the judiciary." 575 U.S. at 445, 449 (citation omitted). Here, the Act is aimed squarely at the application (TikTok) that currently poses a unique national-security threat because of data collection and covert content manipulation, while at the same time authorizing the President to address similar risks in the future should they arise.

b. For similar reasons, petitioners have erred in relying (*e.g.*, ByteDance Appl. 28; Firebaugh Appl. 7) on the statutory exception, under the presidential-designation pathway, for applications with the primary purpose of facilitating product, business, or travel reviews. See Act § 2(g)(2)(B), 138 Stat. 958. The Court in *Humanitarian Law Project* found salutary the fact that the statute there applied only to "designated foreign terrorist organizations" and "displayed a careful balancing of interests in creating limited exceptions" because it showed that "Congress has been conscious of its own responsibility to consider how its actions may implicate constitutional concerns." 561 U.S. at 35-36. Here too, the Act applies only to TikTok and other applications identified by the President under statutory criteria, and Congress carefully balanced those interests in creating a limited exception for applications that do not at the moment (and are unlikely in the future to) present the same national-security risks as TikTok.

Similarly, in *Burson* v. *Freeman*, 504 U.S. 191 (1992), the Court upheld a 100-foot "campaign-free zone" around polling places, with a plurality finding that the restriction was narrowly tailored to further a compelling interest in battling "voter intimidation and election fraud." *Id.* at 206. The plurality rejected the argument that the statute was underinclusive because it restricted only campaigning and not other types of speech, explaining that the State had before it "ample evidence that political candidates have used campaign workers to commit voter intimidation or electoral fraud" but "no evidence" that "other forms of solicitation" were used "to commit such electoral abuses." *Id.* at 207.

Here, Congress had ample evidence of the national-security dangers posed by TikTok in particular and addressed those dangers directly, while authorizing the President to designate other applications that might pose similar national-security concerns in the future. As the plurality observed in *Burson*, "[t]he First Amendment does not require [the government] to regulate for problems that do not exist." 504 U.S. at 207. At the same time, the First Amendment does not prohibit Congress from authorizing the President to regulate similar problems if they should come into existence in the future.

c. Petitioners have suggested (*e.g.*, ByteDance Appl. 31-33) that the Act's provision allowing the Executive Branch to designate other foreign-controlled applications is itself a less-restrictive means of furthering the government's national-security interests because it supposedly provides more process—specifically, public notice and a public report to Congress. Act § 2(g)(3)(B), 138 Stat. 959. That suggestion lacks merit. As the court of appeals observed, ByteDance "received more process than would a company coming under the generally ap-

plicable provisions," given that it "participated in a prolonged negotiation with the Executive that featured numerous meetings and several proposals" and "received individualized consideration by the Congress prior to being required to divest." J.A. 59.

Petitioners also have incorrectly asserted that the presidential-designation pathway is less restrictive because it entails "different *substantive* standards" for regulation. ByteDance Appl. 32. Specifically, petitioners have asserted that ByteDance would not qualify as being "controlled by a foreign adversary"—and thus could not be regulated at all—under the presidential-designation pathway because Yiming Zhang, one of ByteDance's Chinese-national founders who owns 21 percent of the company, now resides in Singapore. See *ibid.* That assertion is both immaterial and incorrect.

It is immaterial because Congress determined, after years of study, that the PRC could exercise control over TikTok in particular in ways that threatened national security—and acted to directly address that known concern. That Congress might have adopted more general criteria for the President to apply in the future with respect to other, as-yet-unidentified entities does not bear on the tailoring of Congress's action with respect to TikTok. Cf. J.A. 42, 56, 58.

Petitioners' assertion is in any event incorrect: Under the presidential-designation pathway, a company qualifies as being "controlled by a foreign adversary" if it meets any of several *disjunctive* criteria—only one of which is that a foreign person "domiciled in" a "foreign adversary country" own at least 20 percent of the company. Act § 2(g)(1), 138 Stat. 958. Even assuming that the law would recognize Zhang as a bona fide domiciliary of Singapore and not the PRC, ByteDance would

nevertheless qualify as being "controlled by a foreign adversary" under one or more of the *other* statutory criteria. For instance, ByteDance is "headquartered in" China, which is sufficient on its own. Act § 2(g)(1)(A), 138 Stat. 958; see J.A. 10; J.A. 212 (House Report 3) (explaining that ByteDance is "founded and headquartered in Beijing"). ByteDance also is "subject to the direction or control of" Chinese persons domiciled in China (in particular, Chinese Communist Party officials), which likewise is sufficient on its own. Act § 2(g)(1)(C), 138 Stat. 958; see J.A. 212 (House Report 3).

d. Petitioners have suggested (*e.g.*, ByteDance Appl. 2, 40; Firebaugh Appl. 2, 15-16, 36-37) that the national-security harms identified by the Executive and Legislative Branches are speculative. But as this Court has observed, "[i]n this [national-security and foreign-policy] context, conclusions must often be based on informed judgment rather than concrete evidence, and that reality affects what [courts] may reasonably insist on from the Government." *Humanitarian Law Project*, 561 U.S. at 34-35. This Court also has cautioned that overly intrusive "'judicial inquiry into the national-security realm raises concerns for the separation of powers,'" especially given that "'when it comes to collecting evidence and drawing inferences' on questions of national security, 'the lack of competence on the part of the courts is marked.'" *Trump* v. *Hawaii*, 585 U.S. 667, 704 (2018) (brackets and citations omitted); see pp. 38, 42, *supra*. And even in contexts not involving national security, "courts must accord substantial deference to the predictive judgments of Congress." *Turner I*, 512 U.S. at 665 (plurality op.); see *Columbia Broadcasting System, Inc.* v. *Democratic National Committee*, 412 U.S. 94, 103 (1973).

Here, Congress and the Executive Branch determined that ByteDance's ownership and control of TikTok pose an unacceptable threat to national security because that relationship could permit a foreign adversary government to collect intelligence on and manipulate the content received by TikTok's American users, even if those harms had not yet materialized. That risk assessment is "entitled to deference." *Humanitarian Law Project*, 561 U.S. at 33; see *id.* at 35 ("The Government, when seeking to prevent imminent harms in the context of international affairs and national security, is not required to conclusively link all the pieces in the puzzle before [the Court] grant[s] weight to its empirical conclusions."). And the political Branches determined that the risk was particularly acute because of how the PRC has strategically "pre-positioned" itself to lie in wait and inflict national-security harms on the United States when the time is ripe. See J.A. 41-42 (finding the government's concerns "well founded, not speculative" based on evidence about the PRC's past actions). In these circumstances, "[t]he Government 'need not wait for a risk to materialize' before acting"; instead, Congress is permitted to prophylactically act to protect the American public from those foreseeable harms. J.A. 41; see J.A. 85 (Congress need not delay until "the damage [is] done before taking action to avert it.").

e. Finally, the court of appeals correctly rejected (J.A. 44) petitioners' reliance on *Lamont* v. *Postmaster General*, 381 U.S. 301 (1965). *Lamont* held that requiring individuals wishing to receive certain foreign "communist political propaganda" in the mail to specifically identify themselves and request delivery in writing violated the First Amendment. See *id.* at 307. The Court

held that such a requirement would impede "the flow of ideas to the public" because it would "inhibit[]" recipients from requesting the materials. *Id.* at 306-307. Nothing about the Act here would inhibit anyone from posting anything to TikTok or otherwise impede the flow of ideas on TikTok. To the contrary, the Act—by preventing a foreign adversary from covertly manipulating the content on TikTok—would facilitate, not impede, the organic flow of ideas. See J.A. 43; cf. *NetChoice*, 603 U.S. at 732-733. The First Amendment obviously would forbid the United States from coercing TikTok into covertly manipulating content to serve the government's own ends. See *NRA* v. *Vullo*, 602 U.S. 175, 190 (2024); cf. *Murthy* v. *Missouri*, 603 U.S. 43, 98-99 (2024) (Alito, J., dissenting). Yet on petitioners' view, the First Amendment *requires* permitting China—a foreign adversary—to do just that. That makes no sense.

4. The classified record further confirms that the Act satisfies even strict scrutiny

The court of appeals relied solely on the public record in denying the petitions for review, see J.A. 64-65 & n.11, and the judgments below may be affirmed on that basis. That said, the classified record describes the threat landscape in more detail and thus lends further support to the conclusions that the government's national-security interests are compelling and that the Act reflects the least restrictive means of achieving those interests. See, *e.g.*, Blackburn Decl. ¶¶ 10-13, 33-35, 52-54, 57, 60-61, 63, 77, 81-89; Vorndran Decl. ¶¶ 7-9, 39-40; Newman Decl. ¶¶ 83, 92, 102-106.

* * * * *

TikTok is undoubtedly "an immensely popular platform" in the United States. J.A. 38. "And yet, in part

precisely because of the platform's expansive reach, Congress and multiple Presidents determined that divesting it from the PRC's control is essential to protect our national security." J.A. 91. That divestiture requirement is narrowly tailored to serve Congress's compelling interests in avoiding vast data collection and covert content manipulation by the Chinese government. And the Act leaves all speech on the platform unrestricted—and will "maintain[] the app and its algorithm for American users," J.A. 92—so long as TikTok is freed from control by a foreign adversary. The Constitution does not prevent Congress from taking that critical and targeted step to protect our Nation's security.*

---

* If this Court concludes that petitioners are entitled to relief, it should limit any relief to those provisions of the Act that directly involve ByteDance and TikTok. For example, petitioners would obtain full relief from declaratory or injunctive relief limited to Section 2(g)(3)(A), which specifically designates ByteDance, TikTok, and related entities as involving a "foreign adversary controlled application" subject to the Act. Act § 2(g)(3)(A)(i)-(iv), 138 Stat. 958-959. There is no basis to address the validity or enjoin enforcement of any other provisions of the Act, including the provisions authorizing the President to designate entities in the future, § 2(g)(3)(B), 138 Stat. 959. See *Califano* v. *Yamasaki*, 442 U.S. 682, 702 (1979) ("[I]njunctive relief should be no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs."); see also Act § 2(e), 138 Stat. 957 (severability clause).

CONCLUSION

The judgments of the court of appeals should be affirmed.

Respectfully submitted.

ELIZABETH B. PRELOGAR
Solicitor General
BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
EDWIN S. KNEEDLER
Deputy Solicitor General
SOPAN JOSHI
Assistant to the Solicitor General
MARK R. FREEMAN
SHARON SWINGLE
DANIEL TENNY
CASEN B. ROSS
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys

DECEMBER 2024

APPENDIX

TABLE OF CONTENTS

APPENDIX

The Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, Div. H, 138 Stat. 955, provides:

SEC. 1. SHORT TITLE

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

SEC. 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.

SEC. 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.