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

REPLY BRIEF FOR THE RESPONDENT

ELIZABETH B. PRELOGAR
Solicitor General
Counsel of Record
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Constitution and statutes:

Miscellaneous:

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

REPLY BRIEF FOR THE RESPONDENT

No one disputes that the People's Republic of China (PRC) seeks to undermine U.S. interests by amassing sensitive data about Americans and engaging in covert and malign influence operations. No one disputes that the PRC pursues those goals through ostensibly private companies subject to its control and by pre-positioning assets in the United States to deploy at opportune moments. And in light of those realities, no one can seriously dispute that the PRC's control of TikTok through ByteDance represents a grave threat to national security: TikTok's collection of reams of sensitive data

about 170 million Americans and their contacts makes it a powerful tool for espionage, and TikTok's role as a key channel of communication makes it a potent weapon for covert influence operations. So long as TikTok remains subject to the PRC's control, the PRC could use those weapons against the United States at any time—for example, at a pivotal moment during a crisis.

The Act is the culmination of a years-long effort by Congress and the Executive Branch to address that acknowledged threat. After years of negotiations, the Executive Branch concluded that ByteDance's proposed mitigation measures were insufficient because they would not eliminate the PRC's access to Americans' data or its control over TikTok—and, more fundamentally, because the Executive Branch could neither trust ByteDance to comply nor detect noncompliance before it was too late. After extensive briefings, Congress agreed and adopted a targeted solution requiring ByteDance to effect a divestiture that frees TikTok from the PRC's control—the same solution identified by the Executive Branch under two Presidents as necessary to resolve the national-security risks.

That divestiture requirement is entirely consistent with the First Amendment and with our Nation's tradition of barring or restricting foreign control of communications channels and other critical infrastructure. In arguing otherwise, petitioners portray the Act as an effort to suppress disfavored views. But nothing in the Act would prevent a post-divestiture TikTok from presenting exactly the same content in exactly the same manner. The Act targets *control by a foreign adversary*, not protected speech.

Petitioners object that the Act is not sufficiently tailored because it singles out TikTok and because Con-

gress purportedly failed to consider less-restrictive alternatives. But Congress permissibly concluded that TikTok's unique nature and scale make it a unique threat. The years of executive and legislative process that preceded the Act refute any suggestion that Congress failed to consider alternatives. And petitioners err in asserting that Congress was required to trust ByteDance to comply with an incomplete and impossible-to-enforce mitigation plan; to rely on ineffective disclosures; or to defer action until the profound threat posed by the PRC's control of TikTok ripened into irreversible national-security harms. The Act satisfies any level of First Amendment scrutiny, and this Court should uphold it.

A. The Act Does Not Trigger Heightened First Amendment Scrutiny

The Act does not warrant heightened First Amendment scrutiny because it does not impose a burden on any cognizable First Amendment rights of ByteDance, its U.S. subsidiary, or TikTok's users. Gov't Br. 19-23. Petitioners do not dispute that ByteDance lacks First Amendment rights because it is a "foreign organization[] operating abroad." *Agency for International Development* v. *Alliance for Open Society International, Inc.*, 591 U.S. 430, 436 (2020) (*AOSI*). And petitioners' arguments based on the asserted rights of the U.S. subsidiary and TikTok's users misunderstand the Act's scope and the relevant First Amendment principles.

"[T]he activity centrally addressed by the Act's divestment mandate is that of a foreign nation rather than a domestic speaker." J.A. 66. On its face, the Act regulates only foreign adversary control, not speech by ByteDance's U.S. subsidiary or TikTok's users. Act § 2(a)(1), (c)(1), 138 Stat. 955-957. "[T]he Act is de-

signed to sever ByteDance from the platform but leave untouched" expression by the U.S. subsidiary and TikTok's users "on a post-divestment version of the app." J.A. 74. Nor does the Act otherwise target protected speech. Congress's data-protection goal has nothing to do with expression at all. And Congress's goal of preventing covert manipulation by the PRC targets only *unprotected* expression: A foreign sovereign has no First Amendment right to covertly manipulate a U.S. platform. Gov't Br. 20-21; cf. *Moody* v. *NetChoice, LLC*, 603 U.S. 707, 747 (2024) (Barrett, J., concurring).

ByteDance asserts (Br. 20-22, 36-37) that its U.S. subsidiary engages in expressive editorial activity. As a factual matter, it is wrong to suggest that the subsidiary made the specific "'editorial choice' to use [ByteDance's] recommendation engine." *Id.* at 36 (brackets and citation omitted). ByteDance, not the subsidiary, created the algorithm and *requires* its use. See, *e.g.*, J.A. 8-10; J.A. 649 (¶¶ 76, 78); J.A. 672-673, 686 (¶¶ 12, 15, 75). That does not ignore corporate separateness (ByteDance Br. 22); it simply recognizes that unlike individuals such as Jeff Bezos (*id.* at 23-24) or Anita Whitney (Firebaugh Br. 38-39), the wholly owned corporate subsidiary operates the platform subject to ByteDance's (and in turn the PRC's) control. More fundamentally, the Act does not directly regulate the U.S. subsidiary's expression. "[T]he company could maintain the same editorial policies"—and could even choose to deploy the same algorithm without being compelled to do so—"on a post-divestment version of the app." J.A. 74.

Petitioners emphasize that divestiture would, as a practical matter, result in indirect effects on the U.S. subsidiary's editorial expression and the speech sent or received by TikTok's users. If ByteDance refuses to di-

vest (because, for example, the PRC will not let it), then TikTok will cease to be available in the United States. Firebaugh Br. 20-21. If ByteDance does divest, its former subsidiary will not be able to associate with ByteDance in running the platform (ByteDance Br. 24), and U.S. users will no longer be able to post on a platform controlled by ByteDance (Firebaugh Br. 21-22). And although nothing in the Act would prohibit a post-divestiture TikTok from independently choosing to use exactly the same algorithm, the PRC has restricted the export of that algorithm for use by an entity outside the PRC's control. ByteDance Br. 24; see J.A. 75.

We do not seek to minimize the practical significance of those effects, but petitioners err in assuming they trigger heightened First Amendment scrutiny. The level of scrutiny depends not on the status of the expression in the abstract or the magnitude of a law's practical effects, but instead on whether the challenged law *directly* targets protected speech. A forced divestiture of a social-media platform under the antitrust laws, for example, would have effects similar to the Act: Such a divestiture would preclude the post-divestiture platform from collaborating with its former parent and prevent users from posting on a platform controlled by the parent—thereby likely altering the mix of speech presented. But such a divestiture requirement plainly would not warrant heightened First Amendment scrutiny. See, *e.g.*, *Citizen Publishing Co.* v. *United States*, 394 U.S. 131, 139 (1969) (challenge to newspaper divestiture had "no support from the First Amendment").

So too here. Like a divestiture required by the antitrust laws, the Act's effect on the subsidiary and TikTok users is not materially different from the effect on the bookstore and its customers in *Arcara* v. *Cloud Books,*

Inc., 478 U.S. 697 (1986). There, the closure of the store under a public-health law unquestionably affected speech as a practical matter by requiring the owners to "move their bookselling business to another location," but the Court declined to apply heightened First Amendment scrutiny because the law did not target protected expression. *Id.* at 706.

Petitioners seek to distinguish *Arcara* and analogize this case to *Minneapolis Star* v. *Minnesota Commissioner of Revenue*, 460 U.S. 575 (1983), and *Arkansas Writers' Project, Inc.* v. *Ragland*, 481 U.S. 221 (1987), on the ground that here, "'the Act singles out TikTok'" "and *does so because of* [its] expressive activity." ByteDance Br. 28 (citation omitted); see Firebaugh Br. 50. That is both wrong and misses the point. It is wrong because the Act addresses a specific national-security threat—foreign-adversary control of TikTok—that has nothing to do with protected expression by the U.S. subsidiary or individual TikTok users. And it misses the point because addressing the national-security threat posed by foreign-adversary control of a communications platform that collects sensitive data about 170 million Americans does not present the "danger of abuse" that made the differential tax treatment of certain newspapers and magazines troubling in those cases. *Arkansas Writers*, 481 U.S. at 226. As the Court explained in *Minneapolis Star*, "differential treatment" of media entities does not warrant heightened scrutiny where, as here, it is justified by "some special characteristic" of the regulated entities. 460 U.S. at 585; see J.A. 78. Indeed, Congress often singles out particular foreign-controlled entities in analogous national-security legislation. See American Free Enterprise Chamber of Commerce Amicus Br. 7-15.

Finally, and for similar reasons, the Act is nothing like the laws at issue in *Lamont* v. *Postmaster General*, 381 U.S. 301 (1965), *Whitney* v. *California*, 274 U.S. 357 (1927), or petitioners' various hypothetical laws restricting expressive association between U.S. and foreign speakers. See ByteDance Br. 23-24; Firebaugh Br. 21-22. Those laws *directly* targeted protected expressive activity in the United States; the Act, in contrast, targets only control by a foreign adversary country.

B. Even If Petitioners Had Cognizable First Amendment Claims, The Act Would Warrant Intermediate Scrutiny

Even if the Act triggered heightened First Amendment review, it would warrant only intermediate scrutiny because it is a content-neutral regulation that imposes at most an incidental burden on protected speech. Gov't Br. 23-28; see *United States* v. *O'Brien*, 391 U.S. 367, 375 (1968). Petitioners contend that the Act triggers strict scrutiny because the government's interest in preventing covert manipulation is in their view content-based; because the Act singles out particular entities; because legislators purportedly disapproved of the content or viewpoints reflected on TikTok; and because of the exceptions in the Act's separate provision allowing the President to designate additional covered platforms. All of those arguments lack merit.

1. Petitioners first assert that "the Act 'cannot be justified without reference to the content of the regulated speech.'" ByteDance Br. 25 (citation omitted). Petitioners do not dispute that the data-collection justification has nothing to do with speech. But they maintain that the covert-manipulation justification "plainly 'is related to expression'" because it "'references the content of TikTok's speech.'" *Id.* at 25-26 (brackets and citations omitted); see *id.* at 28. That is doubly wrong.

First, the Act does not target speech "because of the topic discussed or the idea or message expressed." *City of Austin* v. *Reagan National Advertising of Austin, LLC*, 596 U.S. 61, 69 (2022) (citation omitted). It does not, for example, seek to suppress pro-PRC speech, anti-American speech, or any other specific topics or points of view. And the Act does not even seek to suppress "[s]peech that furthers China's interests" (Firebaugh Br. 25). Instead, it bars PRC *control* over TikTok in order to prevent covert manipulation of the platform by a foreign adversary—regardless of the views expressed in the manipulated content. J.A. 80-81; see Gov't Br. 26.

Second, even if preventing covert manipulation by the PRC could somehow be regarded as a content-based justification, it would not be based on the content of any *protected* expression. Again, the Act seeks to prevent the PRC from covertly coercing ByteDance and its U.S. subsidiary to manipulate the TikTok platform. The PRC and ByteDance obviously have no First Amendment right to engage in such manipulation, and petitioners do not argue otherwise. See *AOSI*, 591 U.S. at 436. And TikTok's U.S. subsidiary likewise has no First Amendment right to be coerced by a foreign government into using a manipulated platform.

2. Relatedly, petitioners assert (*e.g.*, ByteDance Br. 26-27) that the Act warrants strict scrutiny because it targets particular entities. But speaker-based distinctions trigger strict scrutiny only if "the legislature's speaker preference reflects a content preference." *Reed* v. *Town of Gilbert*, 576 U.S. 155, 170 (2015) (citation omitted). Here, the Act's "speaker (non)preference is not grounded in a content preference"; instead, it is based on control by a foreign adversary. J.A. 81.

3. Petitioners next invoke (*e.g.*, ByteDance Br. 15-16; Firebaugh Br. 9) a handful of statements by individual legislators to argue the Act was motivated by disagreement with the views expressed on TikTok. But in *O'Brien*, this Court squarely rejected a similar attempt to subject a facially neutral statute to strict scrutiny on the theory that individual legislators' statements suggested their votes were motivated by hostility towards protected expression. 391 U.S. at 384.

Here, moreover, the legislative record refutes petitioners' attempt to impugn Congress's motives. The House Report, for example, focuses overwhelmingly on the dangers posed by TikTok's "data collection practices." J.A. 212; see J.A. 211-220. And to the extent the Report addressed content, it focused on the threat of covert manipulation by the PRC, highlighting "the PRC's conduct of global foreign malign influence operations, including through platforms such as TikTok." J.A. 220. Similarly, Senator McConnell emphasized the dangers of "PRC influence and control" over TikTok and made clear that his concern was "about conduct, not content." J.A. 229. Senator Cantwell likewise emphasized that Congress sought "to prevent foreign adversaries from conducting espionage, surveillance, and malign operations harming vulnerable Americans." J.A. 232.

Particularly when viewed in that context, the statements petitioners cite—such as the observation that "TikTok 'showed dramatic differences in content relative to other social media platforms,'" ByteDance Br. 16 (brackets and citation omitted); Firebaugh Br. 9 (same)—reflect concern about potential covert manipulation by the PRC, not a desire to suppress the referenced content.

4. Finally, petitioners rely (ByteDance Br. 29; Firebaugh Br. 24-26) on the provision of the Act authorizing the President to designate additional covered applications in the future, arguing that the Act's criteria and exceptions discriminate based on content. But those separate (and severable) provisions of the Act are not at issue here. See J.A. 23. What matters for this case is that, after extensive briefings, Congress identified the PRC's control over TikTok as a unique and uniquely well-documented national-security threat, and did so for reasons unrelated to the content of protected speech.

In any event, petitioners err in criticizing the presidential-designation provision, which covers applications that enable sharing of user-generated content while excluding those with the primary purpose of facilitating product, business, or travel reviews. Those criteria simply describe *social-media sites*, which present unique data-collection concerns. For example, although e-commerce and travel-review sites may also collect some user data, cf. ByteDance Br. 43, petitioners do not suggest that they pose the same risks as a social-media platform that occupies users for hours at a time and uses that intensive engagement to collect "keystroke patterns," "activity across devices," "browsing and search history," "location data," "image and audio information" such as "faceprints and voiceprints," and data about a user's contacts, social network, and private messages. J.A. 38-39. Having focused specifically on the acute threat posed by the PRC's control of TikTok, Congress covered other social-media sites as the class of applications most likely to present a similar threat in the future. That choice does not render the Act's presidential-designation provision impermissibly content-based.

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

The Act easily satisfies intermediate scrutiny—and would also satisfy strict scrutiny—because it is narrowly tailored to further the government's compelling interests in protecting Americans' data and preventing the PRC from covertly manipulating TikTok. Gov't Br. 28-49. Petitioners have little to say about the data-protection interest, which suffices by itself to uphold the Act. Petitioners also have no persuasive response to the national-security harms arising from covert content manipulation. And petitioners' arguments ignore the serious risks posed by the PRC's control of TikTok and would hamstring Congress's ability to protect Americans from obvious foreign threats.

1. The Act is narrowly tailored to protect Americans' sensitive data from the PRC

The government has a compelling interest in preventing the PRC from amassing enormous troves of data on tens of millions of Americans. Gov't Br. 29-33. Petitioners barely address that interest. They do not and could not deny that "the PRC has engaged in 'extensive and years-long efforts to accumulate structured datasets'" on Americans. J.A. 34. They do not and could not deny that the PRC pursues those efforts through ostensibly private companies such as ByteDance, including by adopting laws requiring those companies "to grant the PRC full access to their data." J.A. 35. And petitioners do not and could not deny that the vast array of sensitive data that TikTok harvests about 170 million Americans and their contacts would be enormously valuable to the PRC's malign operations against the United States—especially when aggregated with other information that the PRC has obtained, in-

cluding through cyberattacks on Americans. J.A. 38-39; see Former National Security Officials Amicus Br. 4-10. Instead, petitioners insist that the Court should ignore the data-protection interest and that the Act is underinclusive. Both arguments lack merit.

a. Petitioners principally assert that the government "cannot invoke the data-protection interest" because the "legislative record" does not show that "Congress would have passed the Act for data-protection reasons alone." ByteDance Br. 41-42; see Firebaugh Br. 47-48. That is wrong for three reasons.

First, unlike an administrative agency, Congress is not required to assemble any particular "record" before legislating. "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." *Sable Communications of California, Inc.* v. *FCC*, 492 U.S. 115, 133 (1989) (Scalia, J., concurring). And petitioners cite no precedent for employing the sort of counterfactual analysis they urge in a First Amendment challenge to an Act of Congress. Gov't Br. 36.

Second, and in any event, the counterfactual inquiry petitioners propose applies only when the challenged action is based in part on an *impermissible* motive. Gov't Br. 36-37. Here, the interest in preventing covert content manipulation by the PRC is at minimum permissible. See pp. 17-19, *infra*. Even if that interest would not by itself suffice to sustain the Act, it poses no obstacle to upholding the Act based on the data-protection interest. See, *e.g.*, *Heffron* v. *International Society for Krishna Consciousness, Inc.*, 452 U.S. 640, 649, 650 n.13 (1981) (upholding statute based on "the principal justification asserted by the State" without

addressing whether the State's other asserted interests were "constitutionally sufficient").

Third, this would be a particularly inappropriate case for applying the novel counterfactual analysis petitioners propose. The House Report focuses overwhelmingly on data protection, see J.A. 211-220; the Act passed by large bipartisan majorities, see 170 Cong. Rec. H1170 (daily ed. Mar. 13, 2024) (352-65); 170 Cong. Rec. S2992 (daily ed. Apr. 23, 2024) (79-18); and lawmakers who objected to the Act disputed only the covert-manipulation interest, not the data-protection one, *e.g.*, 170 Cong. Rec. S2968 (Sen. Markey). There is thus every reason to think that Congress would have adopted the Act based on the data-protection interest alone.

Petitioners assert (Firebaugh Br. 48) that the Act cannot be sustained based on data protection because a qualified divestiture must preclude any ongoing cooperation with former foreign-adversary-controlled affiliates concerning not only "data sharing" but also "the operation of a content recommendation algorithm." Act § 2(g)(6)(B), 138 Stat. 959. But that provision simply confirms that Congress had two national-security concerns in mind and was addressing the shortcomings with ByteDance's proposed national security agreement, see J.A. 214; it does not undermine the point that the Act may be sustained on the data-protection rationale. Gov't Br. 35-37. And at a minimum, the data-protection interest would be sufficient to uphold the Act aside from that (severable) provision, which petitioners have not separately challenged.

b. Petitioners also argue that the Act is underinclusive with respect to data protection because it covers only TikTok and (under the presidential-designation

pathway) certain other social-media applications, even though other types of applications also collect user data. ByteDance Br. 42-44; Firebaugh Br. 48-50. But even under strict scrutiny, "the First Amendment imposes no freestanding 'underinclusiveness limitation.'" *Williams-Yulee* v. *Florida Bar*, 575 U.S. 433, 439 (2015) (citation omitted). Underinclusiveness is a problem only if it raises "doubts about whether the government is in fact pursuing the interest it invokes." *Id.* at 448 (citation omitted). And the Act here raises no such doubts. Gov't Br. 32-33.

To the contrary, Congress considered evidence that TikTok collects data on an unsurpassed scale and that ByteDance has a history of abusing that data (by, for example, tracking U.S. journalists). See, *e.g.*, J.A. 37; J.A. 216-219 (House Report); J.A. 232 (Sen. Cantwell); J.A. 659-661 (¶¶ 20, 22, 27, 29, 32); J.A. 695-697 (¶ 95). Petitioners make no showing that Congress had before it evidence that foreign-controlled e-commerce or other sites collect and abuse similar data on a similar scale. Congress permissibly concluded that TikTok poses a unique threat; that other social-media applications might in the future pose similar threats; but that it would be premature to regulate other types of applications. Nothing about those determinations provides any reason to doubt that protecting Americans' sensitive data from the PRC is a bona fide and sufficient basis for the Act. Instead, it shows that Congress "displayed a careful balancing of interests" and was "conscious of its own responsibility to consider how its actions may implicate constitutional concerns." *Holder* v. *Humanitarian Law Project*, 561 U.S. 1, 35-36 (2010).

c. The Act is narrowly tailored to address the data-protection interest. It provides for divestiture to elimi-

nate the PRC's ability to access TikTok data, situating the Act within the "well-established practice of placing restrictions on foreign ownership or control where it could have national security implications." J.A. 44; see Gov't Br. 33-35.

Petitioners assert (ByteDance Br. 46; Firebaugh Br. 51) that Congress could simply have prohibited sharing data with the PRC. But it is naïve to suggest that Congress could trust ByteDance to comply in good faith with such a restriction. See J.A. 692-694 (¶¶ 86-87, 89-91). ByteDance is subject to laws that allow the PRC to demand "full access to [its] data" and prohibit ByteDance from revealing such access. J.A. 35; J.A. 676 (¶ 24). And the Chinese government has a documented history of collecting data through hacking operations that violate U.S. laws, J.A. 33-34; there is little reason to think the PRC would be deterred by a prohibition on accessing data held by a company subject to its control.

For similar reasons, petitioners err in invoking (ByteDance Br. 46) ByteDance's proposed national security agreement. That proposal would not have prevented ByteDance (and thus the PRC) from accessing Americans' sensitive data. Gov't Br. 33-34. More fundamentally, the First Amendment does not require the government to rely on "a potential agreement with a party that it d[oes] not trust"—particularly when that party is subject to a foreign adversary's control and the government lacks "the resources or the capability to catch violations." J.A. 692 (¶ 86).

The government's lack of trust in ByteDance is well-founded. "Public reporting," for example, revealed that "ByteDance employees abused U.S. user data, even after the establishment" of some of the protections contemplated in the proposal. J.A. 695 (¶ 95(a)). Similarly,

leaked "audio recordings" indicated that "ByteDance retained considerable control and influence over" the entity that purported to provide independent safeguards for U.S. users' data. *Ibid.*; see J.A. 37; see also, *e.g.*, J.A. 232 (Sen. Warner) ("Those who suggest that the United States can address the data security and foreign influence risk of TikTok through traditional mitigation measures have not been following TikTok's long track record of deceit and lack of transparency.").

Finally, "[r]equiring TikTok to disclose the potential data-collection risks to users" (Firebaugh Br. 51) is not a viable alternative. The government has publicly highlighted TikTok's data-security risk for years, yet usage of the application—and corresponding data collection—has only continued to grow. See J.A. 214-220. Petitioners provide no reason to think that the sort of generalized disclosure they contemplate would be any more effective. They also ignore that the United States has a compelling interest in preventing the PRC from exploiting TikTok's user data even if individual users would choose to disregard that risk. And the disclosure petitioners posit would do nothing to address TikTok's collection of non-user data or the PRC's ability to combine TikTok data with other data, including information obtained through data breaches and cyber espionage. J.A. 34-42.

2. The Act is narrowly tailored to prevent the PRC from covertly manipulating TikTok

The Act is also narrowly tailored to serve the government's compelling interest in preventing a foreign adversary like the PRC from controlling a key communications channel in the United States, which the PRC could use to conduct a covert influence operation at any time. Gov't Br. 37-40. Petitioners' contrary arguments

mischaracterize the government's interest and invoke alternative measures that would leave TikTok open to PRC manipulation.

a. Petitioners observe that the government does not have a compelling interest in "correcting" the mix of speech on TikTok. But as the court of appeals emphasized, the Act does not seek to "suppress content or require a certain mix of content"; instead, it targets "the PRC's ability to manipulate content covertly" in order to harm the United States. J.A. 30. Such covert foreign manipulation is not protected by the First Amendment, and the national-security harms would arise from the *fact* of such manipulation. Gov't Br. 25-26; J.A. 79-81.

Petitioners assert that the government does not have a compelling interest in "*preventing* Americans from *potentially choosing* to disseminate content at a foreign government's behest." ByteDance Br. 35. That again mischaracterizes the relevant interest: The concern is not that the U.S. subsidiary will independently *choose* to amplify or suppress particular content; it is that *the PRC* will do so by directing covert manipulation of the algorithm, which the subsidiary is compelled to use. The Act's divestiture provision precisely targets that concern by freeing the subsidiary from the PRC's control while leaving it free to disseminate any content it wishes.

b. Ultimately, ByteDance does not deny that the government has a compelling interest in protecting Americans from a communications platform "that a foreign government may have *covertly* influenced." ByteDance Br. 35. But the Firebaugh petitioners appear to assert (Br. 29-47) that the government lacks "a legitimate interest in countering" even "covert content manipulation by the PRC." J.A. 43. As the court of appeals

explained, that argument is "profoundly mistaken." *Ibid.*

It is of course true that "[t]his country has no history or tradition of banning Americans' speech because of concerns that foreign governments might benefit from it or add their own voices to it." Firebaugh Br. 33. But the Act does no such thing. Unlike the real and hypothetical laws on which petitioners rely (*id.* at 34-37), the Act neither seeks to suppress any American's speech nor to prevent any American from receiving speech from abroad—including PRC propaganda. Instead, it simply seeks to prevent the PRC from controlling a platform that holds itself out as "today's quintessential marketplace of ideas" (*id.* at 3) and using it as a covert vector for the PRC's efforts to undermine the United States. By preventing a foreign adversary government from secretly manipulating a U.S. communications platform used by 170 million Americans, "the Act actually vindicates the values that undergird the First Amendment." J.A. 43.

c. Petitioners' assertion (ByteDance Br. 38) that Congress was not genuinely concerned about "the 'covert' nature of any content manipulation" strains credulity. The record reflects Congress's concern that although TikTok purports to be independent, it "can be used by [the PRC]" to "push misinformation, disinformation, and propaganda"—activities that, by definition, are done covertly. J.A. 211. The House Report, for example, recounts concerns about "clandestine[]" manipulation, J.A. 220—including the FBI Director's warning that the PRC could use TikTok "for influence operations," J.A. 217 (citations omitted); see, *e.g.*, J.A. 229 (Sen. McConnell) (rejecting TikTok's "claim that what [TikTok] shows young Americans is what they want to

see, not what the PRC wants"); J.A. 232 (Sen. Warner) ("[TikTok] could be covertly manipulated to serve the goals of an authoritarian regime.").

d. Just as the Act is narrowly tailored to protect Americans' data, it is also narrowly tailored to prevent covert manipulation by the PRC. Again, the Act directly targets the relevant threat—foreign-adversary control—and only that threat. Gov't Br. 40-41. Again, petitioners offer disclosure and ByteDance's proposed "national security agreement" as less-restrictive alternatives. ByteDance Br. 45-47; Firebaugh Br. 41-42. And again, neither alternative would adequately address the government's compelling national-security interest.

Petitioners assert that Congress should have mandated a "conspicuous warning on the TikTok platform" stating that "'The Government believes there is a risk that China may coerce TikTok to covertly manipulate the information received by Americans.'" ByteDance Br. 39-40 (brackets, citation, and ellipsis omitted); see *id.* at 45. But such a generic, standing disclosure would be patently ineffective because it would not reveal whether any *particular* content on TikTok was appearing (or not appearing) organically or because of the PRC's manipulation. "The idea that the Government can simply use speech of its own to counter the risk of content manipulation by the PRC is likewise naïve." J.A. 54.

ByteDance's proposed national security agreement was also insufficient. Indeed, it did not even purport to provide a mechanism to detect content manipulation. Petitioners' declarant described the purpose of the source-code review as the detection of "malicious code," J.A. 434, not "to inspect how the recommendation algo-

rithm makes decisions," J.A. 719. Any effort to identify content manipulation in real time would also be infeasible; the source code changes 1000 times per day, and petitioners themselves maintain that it would take expert engineers "several years" to "gain sufficient familiarity with the source code," ByteDance Br. 14 (citation omitted). That concession belies their assertion that third-party monitoring would be an effective check.

3. Petitioners' remaining arguments lack merit

Petitioners' remaining arguments improperly minimize the compelling national-security interests at stake and demand far more from Congress than this Court's precedents require.

a. Petitioners emphasize (*e.g.*, ByteDance Br. 3) that the government has not identified a documented instance of the PRC's accessing TikTok's data on U.S. users or manipulating the U.S. platform. But such covert activities are by their very nature difficult to document and prove. Just as the "inherent features of the PRC, ByteDance[,] and the TikTok platform would have greatly inhibited the U.S. government's ability to detect violations" of the proposed national security agreement, J.A. 686 (¶ 76), they would also make it difficult to detect if covert intelligence operations are occurring within a tightly integrated network of companies controlled by the PRC.

More fundamentally, "Congress did not need to wait for the risk" of data collection and covert manipulation by the PRC "to become realized and the damage to be done." J.A. 85. The government has a compelling interest in addressing serious national-security threats *before* they ripen into irreversible national-security harms. A foreign adversary's control over a potent tool of espionage and manipulation plainly qualifies as such a

threat. And Congress's interest in addressing that threat is particularly compelling given the PRC's "strategy of pre-positioning assets for potential use against U.S. interests at pivotal moments." *Ibid.*; see Gov't Br. 4, 29-30.

Petitioners suggest (ByteDance Br. 52; Firebaugh Br. 45-46) that the national-security threats are not sufficiently "imminent" to justify the Act because Congress delayed application of the statute's restrictions for 270 days (with a possible 90-day extension). But Congress was entitled to balance the competing policy goals of protecting national security and allowing time for divestiture. And while ByteDance objects (*e.g.*, Br. 14) that the Act's divestiture period is too short, it does not represent that it has taken any steps toward divestiture in the eight months since the Act's adoption—or for that matter in the four years since President Trump's 2020 orders made clear that divestiture could be required if ByteDance failed to address the government's national-security concerns. Congress reasonably expected that ByteDance could effectuate a divestiture freeing TikTok from the PRC's control—thereby protecting national security while preserving access to the platform in the United States. 3/7/24 House Comm. on Energy and Commerce Tr. 72-73, 129-130, 171-173 (E&C Tr.) (C.A. Doc. 2073185). And that divestiture option will remain available after the Act takes effect. Act § 2(c)(1)(B), 138 Stat. 957.

b. Petitioners object that Congress failed to make "statutory findings" (ByteDance Br. 38) documenting its consideration of alternatives. But Congress is not required to memorialize its reasons for enacting a statute. See *Sable Communications*, 492 U.S. at 133 (Scalia, J., concurring). And petitioners' objection is particularly

misplaced here, where Congress considered the threats posed by TikTok for years, heard directly from TikTok's Chief Executive Officer, received numerous classified and unclassified briefings about the Executive Branch's extended negotiations aimed at identifying a less-restrictive alternative, and specifically considered evidence of the inadequacy of various alternatives. Gov't Br. 6-9; see J.A. 213-214, 219, 711-712; E&C Tr. 10-11, 40-42, 49-50.

c. Finally, petitioners badly miss the mark in attacking (ByteDance Br. 47-51) the court of appeals' evaluation of the record. For example, petitioners argue that the court of appeals erred in accepting "assertions that ByteDance Ltd. is a Chinese company or owned by one." *Id.* at 47-48 (citation omitted). But petitioners' emphasis on *ownership* elides how the PRC can *control* ByteDance. The PRC has a well-documented history of using its laws and embedded Chinese Communist Party committees to force companies operating in China—including the relevant ByteDance affiliates—to carry out the PRC's directives and refrain from disclosing those actions. See J.A. 36, 213, 657-658, 673-676. And ByteDance itself has acknowledged that the PRC can control its ability to export its "proprietary recommendation engine." ByteDance C.A. Br. 24.

Petitioners also complain (ByteDance Br. 49) that the court of appeals relied on "the Government's say-so" in finding that ByteDance has censored content outside of China in response to PRC demands. But the court also relied on ByteDance's conspicuous failure to deny that it has engaged in such PRC-directed conduct. J.A. 47; see Gov't Br. 37-38. And while petitioners assert that "reports in the record demonstrate that TikTok has *not* taken down content in other countries at

China's request," ByteDance Br. 49, their cited source is not a factual representation by ByteDance but instead a political-science professor's opinion that social-media companies generally "comply with local laws." J.A. 760 (¶ 20).

Petitioners also cite the same professor's view that "it is unlikely that China would seek to compel TikTok to turn over user data for intelligence-gathering purposes." ByteDance Br. 50 (quoting J.A. 460 (¶ 16)). But in the "sensitive and weighty" context of "national security and foreign affairs," it is the "evaluation of the facts by the Executive" and "Congress's assessment" that are "entitled to deference"—not the predictions of petitioners' preferred professor. *Humanitarian Law Project*, 561 U.S. at 33-34.

d. In an amicus brief, President-elect Trump takes no position on the First Amendment question on which this Court granted certiorari but urges the Court (Br. 4) to "stay the statute's effective date to allow his incoming Administration to pursue a negotiated resolution." That requested relief is more properly characterized as a temporary injunction and thus is appropriate only if the plaintiff establishes, among other things, a likelihood of success on the merits. See *Roman Catholic Diocese of Brooklyn* v. *Cuomo*, 592 U.S. 14, 16 (2020) (per curiam); *Winter* v. *NRDC, Inc.*, 555 U.S. 7, 32 (2008). Petitioners have not made that showing here—and the President-elect does not argue otherwise.

* * * * *

Congress and the Executive Branch agree that the PRC's control of TikTok through ByteDance poses a profound national-security threat. As the court of appeals recognized, that concern is "well founded, not speculative." J.A. 42. And the Act narrowly targets

that concern by requiring divestiture to sever foreign-adversary control, while allowing exactly the same speech on a post-divestiture TikTok. The First Amendment does not prohibit that critical step to protect our Nation's security.

Respectfully submitted.

ELIZABETH B. PRELOGAR
Solicitor General

JANUARY 2025