United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued September 16, 2024 Decided December 6, 2024

No. 24-1113

TIKTOK INC. AND BYTEDANCE LTD.,
PETITIONERS

v.

MERRICK B. GARLAND, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES,
RESPONDENT

Consolidated with 24-1130, 24-1183

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

---

Andrew J. Pincus argued the cause for TikTok Petitioners. With him on the briefs were *Avi M. Kupfer*, *Alexander A. Berengaut*, *David M. Zionts*, *Megan A. Crowley*, and *John E. Hall*.

Jeffrey L. Fisher argued the cause for Creator Petitioners. With him on the briefs were *Ambika Kumar*, *Tim Cunningham*,

Xiang Li, *Elizabeth A. McNamara*, *Chelsea T. Kelly*, *James R. Sigel*, *Adam S. Sieff*, and *Joshua Revesz*.

Jacob Huebert and *Jeffrey M. Schwab* were on the briefs for petitioner BASED Politics, Inc.

David Greene was on the brief for *amici curiae* Electronic Frontier Foundation, et al. in support of petitioners.

Jameel Jaffer and *Eric Columbus* were on the brief for *amici curiae* the Knight First Amendment Institute at Columbia University, et al. in support of petitioners.

Edward Andrew Paltzik and *Serge Krimnus* were on the brief for *amicus curiae* HungryPanda US, Inc. in support of petitioners.

Matt K. Nguyen, *Travis LeBlanc*, *Robert H. Denniston*, *Kathleen R. Hartnett*, and *Jamie D. Robertson* were on the brief for *amici curiae* Social and Racial Justice Community Nonprofits in support of petitioners.

Nicholas Reddick and *Meryl Conant Governski* were on the brief for *amici curiae* First Amendment Law Professors in support of petitioners.

Thomas A. Berry was on the brief for *amicus curiae* the Cato Institute in support of petitioners.

Mark Davies, *Ethan L. Plail*, and *Edred Richardson* were on the brief for *amici curiae* Professors Mueller, Edgar, Aaronson, and Klein in support of petitioners.

Aaron D. Van Oort was on the brief for *amicus curiae* Professor Matthew Steilen in support of petitioners.

Daniel Tenny, Attorney, U.S. Department of Justice, argued the cause for respondent. With him on the brief were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, *Brian D. Netter*, Deputy Assistant Attorney General, *Mark R. Freeman*, *Sharon Swingle*, *Casen B. Ross*, *Sean R. Janda*, and *Brian J. Springer*, Attorneys, *Matthew G. Olsen*, Assistant Attorney General for National Security, *Tyler J. Wood*, Deputy Chief, Foreign Investment Review Section, and *Tricia Wellman*, Acting General Counsel, Office of the Director of National Intelligence.

Thomas R. McCarthy was on the brief for *amici curiae* Former National Security Officials in support of respondent.

Joel L. Thayer was on the brief for *amici curiae* Campaign for Uyghurs, et al. in support of respondent.

Joel L. Thayer was on the brief for *amici curiae* Zephyr Teachout, et al. in support of respondent.

Thomas M. Johnson, Jr., *Jeremy J. Broggi*, and *Joel S. Nolette* were on the brief for *amici curiae* Chairman of the Select Committee on the CCP John R. Moolenaar, et al. in support of respondent.

David H. Thompson, *Brian W. Barnes*, and *Megan M. Wold* were on the brief for *amicus curiae* Professor D. Adam Candeub in support of respondent.

Thomas M. Johnson, Jr., *Jeremy J. Broggi*, and *Michael J. Showalter* were on the brief for *amici curiae* Former Chairman of the Federal Communications Commission Ajit V. Pai and Former Assistant Secretary of the Treasury for Investment Security Thomas P. Feddo in support of respondent.

Jonathan Berry, *Michael Buschbacher*, *Jared M. Kelson*, *James R. Conde*, and *William P. Barr* were on the brief for *amicus curiae* American Free Enterprise Chamber of Commerce in support of respondent.

Austin Knudsen, Attorney General, Office of the Attorney General for the State of Montana, *Christian B. Corrigan*, Solicitor General, *Peter M. Torstensen, Jr.*, Deputy Solicitor General, *Jason S. Miyares*, Attorney General, Office of the Attorney General for the Commonwealth of Virginia, *Erika L. Maley*, Solicitor General, *Kevin M. Gallagher*, Principal Deputy Solicitor General, *Steve Marshall*, Attorney General, Office of the Attorney General for the State of Alabama, *Treg Taylor*, Attorney General, Office of the Attorney General for the State of Alaska, *Tim Griffin*, Attorney General, Office of the Attorney General for the State of Arkansas, *Ashley Moody*, Attorney General, Office of the Attorney General for the State of Florida, *Christopher M. Carr*, Attorney General, Office of the Attorney General for the State of Georgia, *Raúl R. Labrador*, Attorney General, Office of the Attorney General for the State of Idaho, *Theodore E. Rokita*, Attorney General, Office of the Attorney General for the State of Indiana, *Brenna Bird*, Attorney General, Office of the Attorney General for the State of Iowa, *Russell Coleman*, Attorney General, Office of the Attorney General for the Commonwealth of Kentucky, *Liz Murrill*, Attorney General, Office of the Attorney General for the State of Louisiana, *Lynn Fitch*, Attorney General, Office of the Attorney General for the State of Mississippi, *Andrew Bailey*, Attorney General, Office of the Attorney General for the State of Missouri, *Michael T. Hilgers*, Attorney General, Office of the Attorney General for the State of Nebraska, *John M. Formella*, Attorney General, Office of the Attorney General for the State of New Hampshire, *Gentner F. Drummond*, Attorney General, Office of the Attorney General for the State of Oklahoma, *Alan Wilson*, Attorney General, Office of the

Attorney General for the State of South Carolina, *Marty J. Jackley*, Attorney General, Office of the Attorney General for the State of South Dakota, *Jonathan Skrmetti*, Attorney General, Office of the Attorney General for the State of Tennessee, and *Sean D. Reyes*, Attorney General, Office of the Attorney General for the State of Utah, were on the brief for *amici curiae* State of Montana, Virginia, and 19 Other States in support of respondent.

Peter C. Choharis and *Arnon D. Siegel* were on the brief for *amicus curiae* the Foundation for Defense of Democracies in support of respondent.

Before: SRINIVASAN, *Chief Judge*, RAO, *Circuit Judge*, and GINSBURG, *Senior Circuit Judge*.

Opinion for the Court filed by *Senior Circuit Judge* GINSBURG.

Opinion concurring in part and concurring in the judgment filed by *Chief Judge* SRINIVASAN.

I. Background 8
A. The TikTok Platform 8
B. The Petitioners 9
C. National Security Concerns 11
D. The Act 15
1. Foreign adversary controlled applications 16
2. Prohibitions 18
3. The divestiture exemption 19
E. Procedural History 20
II. Analysis 20
A. Standing and Ripeness 21
B. The First Amendment 24
1. Heightened scrutiny applies. 24
2. The Act satisfies strict scrutiny. 32
a. The Government's justifications are compelling. 33
(i) National security justifications 33
(ii) Data collection 38
(iii) Content manipulation 42
b. The Act is narrowly tailored. 48
(i) TikTok's proposed NSA 49
(ii) Other options 53
(iii) Overinclusive / underinclusive 55
C. Equal Protection 57
D. The Bill of Attainder Clause 59
E. The Takings Clause 63
F. Alternative Relief 64
III. Conclusion 65

GINSBURG, *Senior Circuit Judge*: On April 24, 2024 the President signed the Protecting Americans from Foreign Adversary Controlled Applications Act into law. Pub. L. No. 118-50, div. H. The Act identifies the People's Republic of China (PRC) and three other countries as foreign adversaries of the United States and prohibits the distribution or maintenance of "foreign adversary controlled applications."[1] Its prohibitions will take effect on January 19, 2025 with respect to the TikTok platform.

Three petitions — filed by ByteDance Ltd. and TikTok, Inc.; Based Politics, Inc.; and a group of individuals ("Creators") who use the TikTok platform — which we have consolidated, all present constitutional challenges to the Act. We conclude the portions of the Act the petitioners have standing to challenge, that is the provisions concerning TikTok and its related entities, survive constitutional scrutiny. We therefore deny the petitions.

---

[1] A foreign adversary controlled application is defined in § 2(g)(3) as "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 [certain procedures].

I. Background

This court has original and exclusive jurisdiction over this case pursuant to Section 3 of the Act. The parties have submitted several evidentiary appendices in support of their positions, including sworn declarations from various experts. In reviewing this material, we consider whether there is a genuine dispute as to any material fact. *Cf.* Fed. R. Civ. P. 56(a), (c)(4). Here, no dispute of "essential facts" stands in the way of our deciding this case on the merits of the parties' legal arguments. *See Cal. ex rel. State Lands Comm'n v. United States*, 457 U.S. 273, 278 (1982); *South Carolina v. Katzenbach*, 383 U.S. 301, 307 (1966).

A. The TikTok Platform

TikTok is a social-media platform that lets users create, upload, and watch short video clips overlaid with text, voice-overs, and music. For each individual viewer, the platform creates a continuous sequence of videos based upon that user's behavior and several other factors, with the aim of keeping that user engaged. The TikTok platform has approximately 170 million monthly users in the United States and more than one billion users worldwide.

What a TikTok user sees on the platform is determined by a recommendation engine, company content moderation decisions, and video promotion and filtering decisions. The recommendation engine is an algorithm that displays videos based upon content metadata and user behavior. It identifies a pool of candidate videos for a user, then scores and ranks those videos using machine-learning models designed to determine which video(s) would be most appealing to the user. The source code for the engine was originally developed by ByteDance, a company based in China that is the ultimate parent of TikTok. According to TikTok, the global TikTok team, which includes

Chinese engineers, "continually develop[s]" the recommendation engine and platform source code. As we explain in more detail below, the recommendation engine for the version of the platform that operates in the United States is deployed to a cloud environment run by Oracle Corporation.

Content moderation decisions involve a combination of machine and human actions. According to TikTok every video on the TikTok platform goes through "automated moderation" and if deemed potentially problematic is sent to a human moderator for review. TikTok's Head of Operations and Trust & Safety approves the "community guidelines" that drive content moderation on the platform.

Video promotion (also called "heating") and demotion (also called "filtering") decisions are used to advance TikTok's commercial or other goals. These decisions involve promoting or limiting specific videos on the platform. According to TikTok, each video that is promoted is first reviewed by a human. Review teams are regionalized so that videos promoted in the United States are reviewed by U.S.-based reviewers. With respect to filtering, the platform follows "a set of rules to filter out and disperse certain content."

B. The Petitioners

Three groups of petitioners challenge the Act on constitutional grounds: ByteDance Ltd. and TikTok, Inc.; Based Politics, Inc.; and the self-styled Creators, eight individuals who use the TikTok platform. We refer to the latter two groups collectively as the User Petitioners. Where the corporate structure of ByteDance affects our analysis, we identify the relevant corporate entity by name. Otherwise, we refer generally to the constellation of ByteDance entities as TikTok. Because PRC control of the TikTok platform is central to this case, we

provide the following overview of the relevant corporate relationships.

ByteDance Ltd., the ultimate parent company of TikTok, is incorporated in the Cayman Islands. The Government characterizes ByteDance as headquartered in China and ByteDance acknowledges that it has significant operations there.[2] ByteDance provides more than a dozen products through various operating subsidiaries, including Douyin, which is the counterpart to TikTok in China. The company was founded by Yiming Zhang, a Chinese national. Zhang retains 21 percent ownership of the company.

TikTok Ltd. is a wholly owned subsidiary of ByteDance and is also incorporated abroad. TikTok Ltd. operates the TikTok platform globally, except in China. The Government refers to TikTok entities that operate the platform outside the United States as "TikTok Global" and its U.S. operations as "TikTok US."

TikTok Ltd. wholly owns TikTok LLC, which in turn wholly owns TikTok, Inc., a California corporation that provides the TikTok platform to users in the United States. According to a TikTok declarant, TikTok's "U.S. application and global application are highly integrated," and the "global TikTok application itself is highly integrated with ByteDance." Because the TikTok "platform and the content [are] global, the teams working on the platform, and the tools they use, necessarily must be, as well." According to TikTok, one of ByteDance's roles is "development of portions of the computer code that runs the TikTok platform." In the Government's view, TikTok "would try to comply if the PRC asked for specific actions to be taken to manipulate content for

[2] We use "China" when referring to the country and PRC when referencing its government.

censorship, propaganda, or other malign purposes on TikTok US."

TikTok U.S. Data Security Inc. (TTUSDS) is a wholly owned subsidiary of TikTok, Inc., incorporated in Delaware. TikTok created TTUSDS to limit ByteDance's access to the data of TikTok's users in the United States and to monitor the security of the platform. TikTok represents that TTUSDS employees are separated from other TikTok employees, and that it partnered with Oracle to migrate the U.S. version of the TikTok platform into a cloud environment run by Oracle. TikTok also represents that TTUSDS and Oracle review updates to the platform made by ByteDance's non-TTUSDS employees, and that Oracle has full access to TikTok's source code. According to TikTok, TTUSDS is also responsible for deploying the recommendation engine in the United States, and TTUSDS signs off on any decision to promote or demote content in the United States.

C. National Security Concerns

As relevant here, the Executive[3] first became concerned about the PRC's influence over TikTok in 2018 when ByteDance relaunched the platform in the United States following its acquisition of Musical.ly. In 2019, upon finding that "foreign adversaries" were "exploiting vulnerabilities in information and communications technology and services," President Trump declared a national emergency. *Securing the Information and Communications Technology and Services Supply Chain*, Exec. Order No. 13873, 84 Fed. Reg. 22689, 22689 (May 15, 2019). Later that year, the Committee on Foreign Investment in the United States (CFIUS), which comprises the heads of several Executive Branch agencies, sent

[3] The Executive refers variously to the President, Executive Branch agencies, including the intelligence agencies, and officials thereof.

a questionnaire to ByteDance about national security concerns related to ByteDance's acquisition of Musical.ly. Thus began a lengthy investigatory process that culminated on August 1, 2020 with CFIUS concluding that TikTok could not sufficiently mitigate its national security concerns and referring the transaction to the President. The President, acting on that referral, ordered ByteDance to divest any "assets or property" that "enable or support ByteDance's operation of the TikTok application in the United States." *Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297, 51297 (Aug. 14, 2020).

President Trump separately invoked his powers under the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act to address "the threat posed by one mobile application in particular, TikTok." *Addressing the Threat Posed by TikTok*, Exec. Order No. 13942, 85 Fed. Reg. 48637, 48637 (Aug. 6, 2020). President Trump prohibited certain "transactions" with ByteDance or its subsidiaries, *id.* at 48638, and the Secretary of Commerce later published a list of prohibited transactions, 85 Fed. Reg. 60061 (Sept. 24, 2020). Litigation ensued, and two courts enjoined the President's prohibitions under the IEEPA as exceeding his authority under that law. *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 102 (D.D.C. 2020); *Maryland v. Trump*, 498 F. Supp. 3d 624, 638, 641–45 (E.D. Pa. 2020).

In 2021, President Biden withdrew President Trump's IEEPA executive order and issued a new one. In the new order, the President identified the PRC as "a foreign adversary" that "continues to threaten the national security, foreign policy, and economy of the United States" through its control of "software applications" used in the United States. *Protecting Americans' Sensitive Data From Foreign Adversaries*, Exec. Order No. 14034, 86 Fed. Reg. 31423, 31423 (June 9, 2021). President

Biden elaborated that "software applications" can provide foreign adversaries with "vast swaths of information from users," and that the PRC's "access to large repositories" of such data "presents a significant risk." *Id.* President Biden directed several executive agencies to provide risk mitigation options, and he asked for recommended "executive and legislative actions" to counter risks "associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary." *Id.* The following year, President Biden signed into law a bill prohibiting the use of TikTok on government devices. *See generally* Pub. L. No. 117-328, div. R, 136 Stat. 5258 (2022).

Litigation regarding President Trump's divestiture order pursuant to CFIUS's referral began when TikTok filed suit in this court challenging the constitutionality of the order. *See* Pet. for Review, *TikTok Inc. v. CFIUS*, No. 20-1444 (2020). At the request of the parties, in February 2021 this court placed that case in abeyance while the new administration considered the matter and the parties negotiated over an alternative remedy that would sufficiently address the Executive's national security concerns.

During 2021 and 2022, TikTok submitted multiple drafts of its proposed National Security Agreement (NSA) and Executive Branch officials held numerous meetings to consider TikTok's submissions. According to TikTok, there were "at least" 14 meetings or calls, nine written presentations by TikTok, and 15 email exchanges in which "CFIUS posed questions related to [TikTok's] operations and the NSA terms." A TikTok declarant describes the negotiations as "protracted, detailed, and productive," and the Government similarly characterizes them as "significant" and "intensive." Also as part of the process, "Executive Branch negotiators engaged in

extensive, in-depth discussions with Oracle, the proposed Trusted Technology Provider, whose responsibility under the proposed mitigation structure included storing data in the United States, performing source code review, and ensuring safety of the operation of the TikTok platform in the United States."

In August 2022, TikTok submitted its last proposal. Although the parties dispute certain details about how to interpret specific provisions, the broad contours of TikTok's proposed NSA are undisputed. Three aspects of the proposal bear emphasis.

First, the proposal purported to give TikTok operational independence from ByteDance by creating a new entity insulated from the influence of ByteDance, namely TTUSDS. The key management personnel of TTUSDS were to be subject to approval by the Government.

Second, the proposed NSA would create three tiers of data to limit the ability of ByteDance to access the data of TikTok's users in the United States. Protected Data generally would encompass personal information about TikTok's U.S. users — such as their usernames, passwords, user-created content, and any other personally identifiable information — unless such data were classified as Excepted Data or Public Data. Sharing of Protected Data with ByteDance would be prohibited except pursuant to limited-access protocols. Excepted Data would include data that platform users authorized to be shared with TikTok or its affiliates; certain defined data fields; and encrypted usernames, phone numbers, email addresses, etc., for routing to the United States. Public Data would include data generally accessible to platform users, as well as any content a user decides to make public. Under the proposed NSA, TikTok could send Excepted Data and Public Data to ByteDance.

Third, the proposal provided for a "trusted third party," Oracle, to inspect the source code, including TikTok's recommendation engine. It also gave the Government authority, under certain circumstances, to instruct TikTok to shut down the platform in the United States, which TikTok calls a "kill switch."

The Executive determined the proposed NSA was insufficient for several reasons. Most fundamentally, certain data of U.S. users would still flow to China and ByteDance would still be able to exert control over TikTok's operations in the United States. The Executive also did not trust that ByteDance and TTUSDS would comply in good faith with the NSA. Nor did the Executive have "sufficient visibility [into] and resources to monitor" compliance. In the Executive's view, divestment was the only solution that would adequately address its national security concerns. TikTok nevertheless voluntarily implemented some of its proposed mitigation measures.

D. The Act

In the months leading to passage of the Act, the Congress conducted a series of classified briefings and hearings regarding the Government's national security concerns. The Congress then debated and passed the Act as one part of a broader appropriations bill, which also included the Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50, div. I (2024), hereinafter the Data Broker Law. The Act and the Data Broker Law include nearly identical definitions of "foreign adversary country" and "controlled by a foreign adversary." Their aims also overlap. Section 2(a) of the Data Broker Law prohibits third party data brokers from transferring "personally identifiable sensitive data of a United States individual" to a foreign adversary country or an entity "controlled by a foreign adversary." The Act complements that

provision by limiting the ability of foreign adversaries to collect data directly through adversary controlled applications.

The Act itself is narrowly constructed to counter foreign adversary control through divestiture. Three aspects of the Act are particularly relevant to this case: (1) the definition of foreign adversary controlled applications, (2) prohibitions in the Act, and (3) the divestiture option.

1. Foreign adversary controlled applications

The Act defines a Foreign Adversary Controlled Application as "a website, desktop application, mobile application, or augmented or immersive technology application that is operated, directly or indirectly" by either of two distinct groups. § 2(g)(3). The first group consists of the ByteDance constellation of entities, including TikTok, which is identified by name. § 2(g)(3)(A). The second group consists of every covered company[4] that is determined by the President to present a

[4] The term "covered company" is defined as "an entity that operates . . . 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

significant threat to national security. Specifically, it includes any "covered company" that:

> (i) is controlled by a foreign adversary;[5] 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

---

application, or augmented or immersive technology application.

§ 2(g)(2)(A). The term excludes, however, entities that operate an "application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." § 2(g)(2)(B).

[5] The term "controlled by a foreign adversary" means a "covered company or other entity" that 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(g)(1). The definition of "foreign adversary country" encompasses China, Russia, Iran, and North Korea. § 2(g)(2) (defining the term by reference to 10 U.S.C. § 4872(d)(2)).

> what assets would need to be divested to execute a qualified divestiture.

§ 2(g)(3)(B).

2. Prohibitions

The Act contains prohibitions, § 2(a), and a "data and information portability" requirement, § 2(b). The prohibitions do not directly proscribe conduct by an entity that owns a foreign adversary controlled application. Instead, they bar others from providing critical support in the United States for such an application. Specifically, the Act makes it "unlawful for an entity to distribute, maintain, or update" a foreign adversary controlled application in any of two ways:

> (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(a)(1).

With respect to TikTok, the prohibitions take effect 270 days after the Act was passed into law, that is, on January 19, 2025. § 2(a)(2)(A). With respect to applications subject to the generally applicable provisions, the prohibitions take effect 270 days after "the relevant determination of the President."

§ 2(a)(2)(B). In both situations, the President can grant a one-time, 90-day extension under specific circumstances not relevant here. § 2(a)(3).

Failure to comply with the Act can result in substantial monetary penalties. § 2(d)(1). To enforce the Act the Attorney General, following an investigation, can file suit in an appropriate district court. § 2(d)(2).

3. The divestiture exemption

Section 2(c) of the Act provides an exemption "for qualified divestitures." That is, the prohibitions do not apply if "a qualified divestiture is executed before the date on which a prohibition under subsection (a) would begin to apply." § 2(c)(1)(A). If a qualified divestiture is executed after that date, then the prohibitions "shall cease to apply." § 2(c)(1)(B). A "qualified divestiture" is defined as a 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.

§ 2(g)(6).

E. Procedural History

This case concerns three petitions challenging the Act that this court consolidated for review. On May 17, 2024 the parties jointly asked this Court to expedite the case. The parties advised that they intended to append evidentiary materials to their briefs. The Government noted that it was evaluating the need to file an ex parte evidentiary submission given the classified material implicated by the case. The petitioners reserved the right to object to any such submission.

The parties ultimately submitted evidence with their briefs. TikTok's submission included several expert declarations as well as a declaration from its Head of Operations and Trust & Safety. The User Petitioners filed declarations underscoring the diverse ways in which they use the TikTok platform. The Government filed declarations explaining its national security concerns and why it found TikTok's proposed NSA insufficient to meet those concerns. TikTok filed rebuttal declarations with its reply brief.

Portions of the Government's brief and evidentiary submission were redacted because they contain classified information. The Government filed a motion requesting leave to file unredacted versions of its brief and supporting evidence under seal and ex parte, which documents the Government later lodged with this court. The petitioners opposed the Government's motion and alternatively moved this court to appoint a special master and issue a temporary injunction in order to mitigate prejudice arising from the Government's classified filings.

II. Analysis

The petitioners seek a declaratory judgment that the Act violates the Constitution and an order enjoining the Attorney

General from enforcing it. Because the petitioners are bringing a pre-enforcement challenge to the Act, we must determine the extent to which this court can consider their claims consistent with the standing aspect of the "case or controversy" requirement of Article III of the Constitution. We conclude that TikTok has standing to challenge those portions of the Act that directly affect the activities of ByteDance and its affiliates. We further conclude that TikTok's challenge to those portions of the Act is ripe.

On the merits, we reject each of the petitioners' constitutional claims. As we shall explain, the parts of the Act that are properly before this court do not contravene the First Amendment to the Constitution of the United States, nor do they violate the Fifth Amendment guarantee of equal protection of the laws; constitute an unlawful bill of attainder, in violation of Article I, § 9, clause 3; or work an uncompensated taking of private property in violation of the Fifth Amendment.

A. Standing and Ripeness

We have an independent duty to assure ourselves that the petitioners and their claims satisfy the requirements of Article III. *Exelon Corp. v. FERC*, 911 F.3d 1236, 1240 (D.C. Cir. 2018). TikTok's claims all relate to how the Act applies to the TikTok platform; it has not, for example, meaningfully developed claims regarding other services provided by other ByteDance subsidiaries. Nor does it claim the generally applicable portions of the Act are unconstitutional as applied to other companies. TikTok instead seeks to enjoin the enforcement of the prohibitions on hosting the TikTok platform, which TikTok contends are unconstitutional irrespective of whether they are imposed based upon the generally applicable framework or upon the TikTok-specific provisions of the Act. At the same time, the User Petitioners claim the Act in its entirety is

"facially invalid under the First Amendment," which need not detain us.[6] Creator Reply Br. 30–31.

"To establish standing for a pre-enforcement challenge, a plaintiff must demonstrate first an intention to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute and, second, that there exists a credible threat of prosecution thereunder." *Muthana v. Pompeo*, 985 F.3d 893, 911 (D.C. Cir. 2021) (cleaned up). This inquiry is slightly more refined in cases that involve the potential future regulation of third parties. To establish standing in such circumstances, a plaintiff must demonstrate it is "likely that the government's regulation . . . of someone else will cause a concrete and particularized injury in fact to the unregulated plaintiff." *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 385 n.2 (2024).

Ripeness is "related" but focuses "on the timing of the action rather than on the parties seeking to bring it." *Navegar, Inc. v. United States*, 103 F.3d 994, 998 (D.C. Cir. 1997). Courts consider (1) hardship to the parties and (2) fitness for judicial resolution when assessing ripeness. *Id.* The purposes of the ripeness doctrine are to avoid abstract argument, promote judicial economy, and ensure an adequate record. *Id.*

TikTok and its claims challenging enforcement of the prohibitions of the Act based upon the TikTok-specific provisions clearly satisfy the requirements respectively for standing and ripeness. The prohibitions based upon those provisions

---

[6] The User Petitioners have not demonstrated that "a substantial number of" the Act's "applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2397 (2024) (cleaned up). Indeed, the core of the Act — its application as to TikTok — is valid for the reasons we explain in this opinion.

take effect by operation of law on January 19, 2025. After that date, third parties that make the TikTok platform available in the United States would run a significant risk of incurring monetary penalties under § 2(d)(1). Even if the Act went unenforced, the risk of penalties alone could cause third parties to suspend support for the TikTok platform, such as by removing it from online marketplaces, and an injunction would prevent that harm. TikTok therefore has Article III standing to pursue its claims.

The ripeness inquiry is likewise straightforward. TikTok risks severe hardship from delayed review, and we have an adequate record on which to resolve the company's challenges to the constitutionality of the TikTok-specific provisions of the Act.

To the extent TikTok seeks to enjoin future enforcement of the prohibitions under the generally applicable track, TikTok does not have standing. Nor if it did would such a request be ripe for judicial review. Recall that applying the prohibitions under the generally applicable framework requires certain procedural steps and a presidential determination pursuant to § 2(g)(3)(B). Those steps include public notice, a description of the national security concern, a classified annex, and a description of assets to be divested. § 2(g)(3)(B)(ii). The President has not invoked those procedures with respect to TikTok (or any other company), and it would be self-evidently premature for the court even to consider a request for an injunction against the President ever doing so. We consequently limit our analysis to the constitutionality of the Act as applied to the TikTok-specific provisions that will go into effect next month.[7]

[7] Having concluded that TikTok has standing, we need not separately analyze whether the User Petitioners have standing to raise the same claims. *See Carpenters Indus. Council v. Zinke*, 854 F.3d 1, 9 (D.C. Cir. 2017) (explaining that "if constitutional standing can be shown

B. The First Amendment

This case requires that we apply longstanding First Amendment principles to somewhat novel facts: A popular social-media platform, subject to the control of a foreign adversary nation, that a statute requires be divested because of national security risks. The issue is made more complex by the web of subsidiaries wholly owned by ByteDance that lie behind the TikTok platform. *See Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2410 (2024) (Barrett, J., concurring) (explaining how foreign ownership and corporate structure can complicate the First Amendment analysis).

We conclude the Act implicates the First Amendment and is subject to heightened scrutiny. Whether strict or intermediate scrutiny applies is a closer question. The relevant portions of the Act are facially content neutral, but the Government arguably based its content-manipulation justification for the Act upon the content on the platform. We think it only prudent, therefore, to assume without deciding that the higher standard applies.

1. Heightened scrutiny applies.

As in most First Amendment cases, the parties spend much of their time debating the appropriate standard of review. The petitioners urge the court to apply strict scrutiny but contend the Act fails intermediate scrutiny as well. The Government suggests we apply only rational basis review, alternatively advocates intermediate scrutiny, but maintains the Act satisfies even strict scrutiny.

---

for at least one plaintiff, we need not consider the standing of the other plaintiffs to raise that claim" (cleaned up)).

Under intermediate scrutiny, the Act complies with the First Amendment "if it 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 Broad. Sys., Inc. v. FCC* (*Turner II*), 520 U.S. 180, 189 (1997) (citing *United States v. O'Brien*, 391 U.S. 367, 377 (1968)). Under strict scrutiny, the Act violates the First Amendment unless the Government can "prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (cleaned up).

We think it clear that some level of heightened scrutiny is required. The question whether intermediate or strict scrutiny applies is difficult because the TikTok-specific provisions are facially content neutral, yet the Government justifies the Act in substantial part by reference to a foreign adversary's ability to manipulate content seen by Americans. No Supreme Court case directly addresses whether such a justification renders a law content based, thereby triggering strict scrutiny. There are reasonable bases to conclude that intermediate scrutiny is appropriate even under these circumstances. We need not, however, definitively decide that question because we conclude the Act "passes muster even under the more demanding standard." *FEC v. Int'l Funding Inst.*, 969 F.2d 1110, 1116 (D.C. Cir. 1992); *see also In re Sealed Case*, 77 F.4th 815, 829–30 (D.C. Cir. 2023) (assuming without deciding that strict scrutiny applied).

At the outset, we reject the Government's ambitious argument that this case is akin to *Arcara v. Cloud Books, Inc.*, 478 U.S. 697 (1986), and does not implicate the First Amendment at all. That case concerned enforcement of "a public health regulation of general application against" an adult bookstore being "used for prostitution." *Id.* at 707.

Enforcement of a generally applicable law unrelated to expressive activity does not call for any First Amendment scrutiny. *Id.* By contrast, the First Amendment is implicated in "cases involving governmental regulation of conduct that has an expressive element," or when a statute is directed at an activity without an expressive component but imposes "a disproportionate burden upon those engaged in protected First Amendment activities." *Id.* at 703–04; *see also Alexander v. United States*, 509 U.S. 544, 557 (1993).

Here the Act imposes a disproportionate burden on TikTok, an entity engaged in expressive activity. The Government concedes, as it must after *NetChoice*, that the curation of content on TikTok is a form of speech. 144 S. Ct. at 2401. Like the social media companies in that case, TikTok delivers a "personalized collection" of content to users and moderates this content pursuant to its community guidelines. *Id.* at 2403–04. The Act plainly "single[s] out" that expressive activity by indirectly subjecting TikTok — and so far, only TikTok — to the divestiture requirement. *Arcara*, 478 U.S. at 707; *cf. Nat'l Rifle Ass'n of Am. v. Vullo*, 602 U.S. 175, 190 (2024) (explaining that "the First Amendment prohibits government officials from wielding their power selectively to punish or suppress speech, directly or (as alleged here) through private intermediaries"). The prohibitions will make it unlawful for any entity to distribute, maintain, or update the TikTok platform in the United States. § 2(a)(1). TikTok can avoid the prohibitions by making a qualified divestiture, § 2(c), but to qualify such divestiture must preclude "any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing," § 2(g)(6)(B). By prohibiting third parties from hosting TikTok until the platform executes this divestiture, the Act singles out TikTok, which engages in expressive activity, for disfavored treatment.

The Government suggests that because TikTok is wholly owned by ByteDance, a foreign company, it has no First Amendment rights. *Cf. Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 591 U.S. 430, 436 (2020) (explaining that "foreign organizations operating abroad have no First Amendment rights"). TikTok, Inc., however, is a domestic entity operating domestically. *See NetChoice*, 144 S. Ct. at 2410 (Barrett, J., concurring) (identifying potential "complexities" for First Amendment analysis posed by the "corporate structure and ownership of some platforms"). The Government does not dispute facts suggesting at least some of the regulated speech involves TikTok's U.S. entities. *See* TikTok App. 811–12, 817–18 (explaining that promoted videos are "reviewed by a U.S.-based reviewer," that an executive employed by a U.S. entity approves the guidelines for content moderation, and that the recommendation engine "is customized for TikTok's various global markets" and "subject to special vetting in the United States").

Nor does the Government argue we should "pierce the corporate veil" or "invoke any other relevant exception" to the fundamental principle of corporate separateness. *Agency for Int'l Dev.*, 591 U.S. at 435–36. We are sensitive to the risk of a foreign adversary exploiting corporate form to take advantage of legal protections in the United States. Indeed, the Government presented evidence to suggest the PRC intentionally attempts to do just that. *See, e.g.*, Gov't App. 33–35 (describing the PRC's hybrid commercial threat and its exploitation of U.S. legal protections for hacking operations). Under these circumstances, however, we conclude that the TikTok-specific provisions of the Act trigger First Amendment scrutiny.

The next question is whether intermediate or strict scrutiny is appropriate, which turns on whether the Act is content

neutral or content based. *See Turner Broad. Sys., Inc. v. FCC* (*Turner I*), 512 U.S. 622, 642 (1994) (explaining that "regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny, because in most cases they pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue" (citation omitted)). A law is content based if it "applies to particular speech because of the topic discussed or the idea or message expressed." *Reed*, 576 U.S. at 163. It is facially content based "if it targets speech based on its communicative content." *City of Austin v. Reagan Nat'l Advert. of Austin, LLC*, 596 U.S. 61, 69 (2022) (cleaned up). A law that "requires an examination of speech only in service of drawing neutral, location-based lines" does not target speech based upon its communicative content. *Id.*; *see BellSouth Corp. v. FCC* (*BellSouth I*), 144 F.3d 58, 69 (D.C. Cir. 1998) (applying intermediate scrutiny to a law that "defines the field of expression to which it applies by reference to a set of categories that might in a formal sense be described as content-based"). Facial neutrality, however, does not end the analysis. Even laws that are facially content neutral are content based if they (a) "cannot be justified without reference to the content of the regulated speech" or (b) "were adopted by the government because of disagreement with the message the speech conveys." *Reed*, 576 U.S. at 164 (cleaned up).

The provisions of the Act before us are facially content neutral because they do not target speech based upon its communicative content. The TikTok-specific provisions instead straightforwardly require only that TikTok divest its platform as a precondition to operating in the United States. On its face, the Act concerns control by a foreign adversary and not "the topic discussed or the idea or message expressed." *City of Austin*, 596 U.S. at 69 (cleaned up).

TikTok insists the TikTok-specific provisions nonetheless require strict scrutiny because they single out a particular speaker. To be sure, laws that "discriminate among media, or among different speakers within a single medium, often present serious First Amendment concerns." *Turner I*, 512 U.S. at 659. "It would be error to conclude, however, that the First Amendment mandates strict scrutiny for any speech regulation that applies to one medium (or a subset thereof) but not others." *Id.* at 660; *see, e.g.*, *BellSouth I*, 144 F.3d at 68 (rejecting argument that a statute "warrants strict First Amendment review because it targets named corporations"). Strict scrutiny "is unwarranted when the differential treatment is justified by some special characteristic of the particular medium being regulated." *Turner I*, 512 U.S. at 660–61 (cleaned up). As of now, the TikTok platform is the only global platform of its kind that has been designated by the political branches as a foreign adversary controlled application. As explained below, the Government presents two persuasive national security justifications that apply specifically to the platform that TikTok operates. "It should come as no surprise, then, that Congress decided to impose [certain restrictions] upon [TikTok] only." *Id.* at 661.

Whether the Act, which is facially content neutral, is subject to strict scrutiny therefore turns upon the Government's justifications for the law. *See Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (stating that a "regulation of expressive activity is content neutral so long as it is justified without reference to the content of the regulated speech" (cleaned up)); *Reed*, 576 U.S. at 164 (explaining that laws are content based if they "cannot be justified without reference to the content of the regulated speech" (cleaned up)); *City of Austin*, 596 U.S. at 76 (explaining that "an impermissible purpose or justification" may render a facially content-neutral restriction content based). The Government offers two national security justifications:

(1) to counter the PRC's efforts to collect great quantities of data about tens of millions of Americans, and (2) to limit the PRC's ability to manipulate content covertly on the TikTok platform. The former does not reference the content of speech or reflect disagreement with an idea or message. *See Ward*, 491 U.S. at 792 (finding justifications offered for a municipal noise regulation content neutral). The Government's explanation of the latter justification does, however, reference the content of TikTok's speech. Specifically, the Government invokes the risk that the PRC might shape the content that American users receive, interfere with our political discourse, and promote content based upon its alignment with the PRC's interests. In fact, the Government identifies a particular topic — Taiwan's relationship to the PRC — as a "significant potential flashpoint" that may be a subject of the PRC's influence operations, and its declarants identify other topics of importance to the PRC. Gov't Br. 22 (quoting Gov't App. 7 (Decl. of Asst. Dir. of Nat'l Intel. Casey Blackburn)); *see also* Gov't App. 9, 22.

At the same time, the Government's concern with content manipulation does not reflect "an impermissible purpose or justification." *City of Austin*, 596 U.S. at 76. On the contrary, the Government's aim is to preclude a foreign adversary from manipulating public dialogue. To that end, the Act narrowly addresses foreign adversary control of an important medium of communication in the United States. Consequently, the Government does not suppress content or require a certain mix of content. Indeed, content on the platform could in principle remain unchanged after divestiture, and people in the United States would remain free to read and share as much PRC propaganda (or any other content) as they desire on TikTok or any other platform of their choosing. What the Act targets is the PRC's ability to manipulate that content covertly. Understood

in that way, the Government's justification is wholly consonant with the First Amendment.

Although we can conceive of reasons intermediate scrutiny may be appropriate under these circumstances, we ultimately do not rest our judgment on those reasons because the Act satisfies "the more demanding standard." *Int'l Funding Inst.*, 969 F.2d at 1116. We therefore assume without deciding that strict scrutiny applies and uphold the law on that basis.[8] Our decision to resolve the case in this way follows a similar approach taken by this and other courts when faced with a government action that would satisfy strict scrutiny. *See In re Sealed Case*, 77 F.4th at 829–30; *United States v. Hamilton*, 699 F.3d 356, 371 (4th Cir. 2012); *OPAL – Bldg. AAPI Feminist Leadership v. Yost*, No. 24-3768, 2024 WL 4441458, at *5 (6th Cir. Oct. 8, 2024); *see also Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293, 298–99 (1984) (assuming without deciding that conduct implicated the First Amendment and upholding a regulation under intermediate scrutiny); *Int'l Funding Inst.*, 969 F.2d at 1116 (assuming without deciding that intermediate scrutiny rather than rational-basis review applied); *United States v. Trump*, 88 F.4th 990, 1008 (D.C. Cir. 2023) (assuming without deciding "that the most demanding scrutiny" applied to an order restricting the speech of the defendant in a criminal trial); *cf. City of Ladue v. Gilleo*, 512 U.S. 43, 53 & n.11 (1994) (conversely assuming

[8] We agree with our concurring colleague that the Government's data-protection rationale "is plainly content-neutral" and standing alone would at most trigger intermediate scrutiny. Concurring Op. 12–13. As we have explained, however, that is not clear for the Government's content-manipulation justification, and no party has identified any portion of the Act to which the data justification alone applies. We therefore assume strict scrutiny applies to our review of the Act in its entirety and consider both justifications under that standard.

without deciding intermediate scrutiny rather than strict scrutiny should be applied, thereby setting "to one side the content discrimination question").

2. The Act satisfies strict scrutiny.

To satisfy strict scrutiny the Government must "demonstrate that a speech restriction: (1) serves a compelling government interest; and (2) is narrowly tailored to further that interest." *In re Sealed Case*, 77 F.4th at 830. "A restriction is narrowly tailored if less restrictive alternatives would not accomplish the Government's goals equally or almost equally effectively." *Id.* (cleaned up). The Act clears this high bar.

We emphasize from the outset that our conclusion here is fact-bound. The multi-year efforts of both political branches to investigate the national security risks posed by the TikTok platform, and to consider potential remedies proposed by TikTok, weigh heavily in favor of the Act. The Government has offered persuasive evidence demonstrating that the Act is narrowly tailored to protect national security. "Given the sensitive interests in national security and foreign affairs at stake," the Government's judgment based upon this evidence "is entitled to significant weight." *Holder v. Humanitarian Law Project*, 561 U.S. 1, 36 (2010). Our deference to the Government's national-security assessment "is redoubled by the repeated acts of" the political branches to address the national security problems presented by the TikTok platform. *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948 (D.C. Cir. 2024). The Act was the culmination of extensive, bipartisan action by the Congress and by successive presidents. It was carefully crafted to deal only with control by a foreign adversary, and it was part of a broader effort to counter a well-substantiated national security threat posed by the PRC. Under

these circumstances, the provisions of the Act that are before us withstand the most searching review.

a. The Government's justifications are compelling.

Recall that the Government offers two national security justifications for the Act: to counter (1) the PRC's efforts to collect data of and about persons in the United States, and (2) the risk of the PRC covertly manipulating content on TikTok. Each constitutes an independently compelling national security interest.

In reaching that conclusion, we follow the Supreme Court in affording great weight to the Government's "evaluation of the facts" because the Act "implicates sensitive and weighty interests of national security and foreign affairs." *Humanitarian Law Project*, 561 U.S. at 33–34; *Trump v. Hawaii*, 585 U.S. 667, 707–08 (2018) (same); *see, e.g.*, *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1162, 1164 (D.C. Cir. 2023) (declining to second-guess the Executive's judgment regarding a national security threat posed by the PRC). At the same time, of course, we "do not defer to the Government's reading of the First Amendment." *Humanitarian Law Project*, 561 U.S. at 34. We simply recognize the comparatively limited competence of courts at "collecting evidence and drawing factual inferences in this area." *Id.* With regard to national security issues, the political branches may — and often must — base their actions on their "informed judgment," which "affects what we may reasonably insist on from the Government." *Id.* at 34–35.

(i) *National security justifications*

The Government provides persuasive support for its concerns regarding the threat posed by the PRC in general and

through the TikTok platform in particular. As Assistant Director of National Intelligence Casey Blackburn explained, the "PRC is the most active and persistent cyber espionage threat to U.S. government, private-sector, and critical infrastructure networks." Its hacking program "spans the globe" and "is larger than that of every other major nation, combined." The PRC has "pre-positioned" itself "for potential cyber-attacks against U.S. critical infrastructure by building out offensive weapons within that infrastructure." Consistent with that assessment, the Government "has found persistent PRC access in U.S. critical telecommunications, energy, water, and other infrastructure." *See China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256, 262–63 (D.C. Cir. 2022) (describing the Government's shift in focus from terrorism to PRC "cyber threats" and the risk posed by use of PRC-connected "information technology firms as systemic espionage platforms"). "The FBI now warns that no country poses a broader, more severe intelligence collection threat than China." *Id.* at 263.

Of particular relevance to the Government's first justification for the Act, the PRC has engaged in "extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations." It has done so through hacking operations, such as by penetrating the U.S. Government Office of Personnel Management's systems 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.

The PRC's methods for collecting data include using "its relationships with Chinese companies," making "strategic investments in foreign companies," and "purchasing large data sets." For example, the PRC has attempted "to acquire sensitive

health and genomic data on U.S. persons" by investing in firms that have or have access to such data. Government counterintelligence experts describe this kind of activity as a "hybrid commercial threat."

The PRC poses a particularly significant hybrid commercial threat because it has adopted laws that enable it to access and use data held by Chinese companies. *See China Telecom (Ams.) Corp.*, 57 F.4th at 263 (describing the legal framework through which the PRC has "augmented the level of state control over the cyber practices of Chinese companies"). For example, the National Security Law of 2015 requires all citizens and corporations to provide necessary support to national security authorities. Similarly, the Cybersecurity Law of 2017 requires Chinese companies to grant the PRC full access to their data and to cooperate with criminal and security investigations.

The upshot of these and other laws, according to the Government's declarants, is that "even putatively 'private' companies based in China do not operate with independence from the government and cannot be analogized to private companies in the United States." Through its "control over Chinese parent companies," the PRC can also "access information from and about U.S. subsidiaries and compel their cooperation with PRC directives." 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." According to Kevin Vorndran, Assistant Director of the FBI's Counterintelligence Division, the PRC endeavors strategically to pre-position commercial entities in the United States that the PRC can later "co-opt." These pre-positioning "tactics can occur over the span of several years of planning and implementation, and they

are one "part of the PRC's broader geopolitical and long-term strategy to undermine U.S. national security."

The PRC likewise uses its cyber capabilities to support its influence campaigns around the world. Those global "influence operations" aim to "undermine democracy" and "extend the PRC's influence abroad." Specifically, the PRC conducts "cyber intrusions targeted to affect U.S. and non-U.S. citizens beyond its borders — including journalists, dissidents, and individuals it views as threats — to counter and suppress views it considers critical of [the PRC]." Notably, the Government reports that "ByteDance and TikTok Global have taken action in response to PRC demands to censor content *outside* of China."

As it relates to TikTok in the United States, the Government predicts that ByteDance and TikTok entities "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 US." The Government says that 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. The former conclusion is evidenced by the fact that the PRC maintains a powerful Chinese Communist Party committee "embedded in ByteDance" through which it can "exert its will on the company." As of 2022, that committee "was headed by the company's chief editor and comprised at least 138 employees at its Beijing office, including senior company managers." The latter conclusion is supported by the fact that TikTok's U.S. operations are "heavily reliant" on ByteDance. As TikTok's declarants have put it, "TikTok in the United States is an integrated part of the global platform" supported by teams "spread across several different corporate entities and countries," and TikTok is "highly integrated with ByteDance."

The Government also identifies several public reports, which were considered by the Congress prior to passing the Act, regarding the risks posed by TikTok.[9] For example, a Government declarant points to "reporting by Forbes Magazine" to illustrate in part why the Government did not trust TikTok's proposed mitigation measures. The reporting suggested "that ByteDance employees abused U.S. user data, even after the establishment of TTUSDS," and drew attention to "audio recordings of ByteDance meetings" that indicated "ByteDance retained considerable control and influence over TTUSDS operations." In its report recommending passage of the Act, a committee of the Congress collected "a list of public statements that have been made regarding the national security risks posed by . . . TikTok." H.R. Rep. No. 118-417, at 5–12 (2024). According to the committee, public reporting suggested that TikTok had stored sensitive information about U.S. persons (including "Social Security numbers and tax identifications") on servers in China; TikTok's "China-based employees" had "repeatedly accessed non-public data about U.S. TikTok users"; ByteDance employees had "accessed TikTok user data and IP addresses to monitor the physical locations of

[9] Although our disposition of this case does not turn upon these reports, the Congress and the President obviously were entitled to consider such materials when deciding whether to define TikTok as a foreign adversary controlled application under the Act. Indeed, we have "approved" the use of similar public materials by the President when making decisions to designate people or entities under various national-security related statutes. *See Zevallos v. Obama*, 793 F.3d 106, 109, 113 (2015) (finding it "clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations" (quoting *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 162 (2003) (regarding designation of an entity as a Specially Designated Global Terrorist))).

specific U.S. citizens"; and PRC agents had inspected "TikTok's internal platform." *Id.* at 7–10.

The resulting judgment of the Congress and the Executive regarding the national security threat posed by the TikTok platform "is entitled to significant weight, and we have persuasive evidence [in the public record] before us to sustain it." *Humanitarian Law Project*, 561 U.S. at 36. The petitioners raise several objections to each national security justification, which we take up next, but the bottom line is that they fail to overcome the Government's considered judgment and the deference we owe that judgment.

(ii) *Data collection*

TikTok disputes certain details about the Government's concern with its collection of data on U.S. persons but misses the forest for the trees. The TikTok platform has more than 170 million monthly users in the United States. It is an immensely popular platform on which users in the United States have uploaded more than 5.5 billion videos in a single year. According to TikTok's "privacy policy," 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). TikTok, *Privacy Policy*, https://perma.cc/E36Q-M3KS (last updated Aug. 19, 2024). 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). *Id.* That is not to mention information that users voluntarily provide, such as name, age,

username, password, email, phone number, social media account information, messages exchanged on the platform and, "with your permission," your "phone and social network contacts." *Id.* TikTok's "privacy policy" also makes clear that it uses these data to "infer additional information" about its users. Given the magnitude of the data gathered by TikTok and TikTok's connections to the PRC, two consecutive presidents understandably identified TikTok as a significant vulnerability. 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." *Addressing the Threat Posed by TikTok*, 85 Fed. Reg. at 48637.

TikTok does not deny that it collects a substantial amount of data on its users. Instead TikTok disputes details about the Government's understanding of its data practices and questions the sincerity of the Government's data justification. At the same time, however, TikTok's own declarants provide support for the Government's concern. They emphasize the integrated nature of the TikTok platform to argue that divestiture would be infeasible. They argue that prohibiting data sharing between TikTok in the United States and "the entities that operate the global platform" would make TikTok uncompetitive with "rival, global platforms." They also acknowledge that, even under TikTok's proposed NSA, ByteDance would continue to have access to some Protected Data on TikTok users in the United States through "limited access protocols." They likewise state that TikTok's proposed NSA "does allow for TTUSDS and Oracle to send 'Excepted Data' to ByteDance."

Set against those statements, TikTok's arguments concerning the specific data collected and TikTok's voluntary data protection efforts fall flat. For example, TikTok quibbles with the Government's stated concern that TikTok collects data

on users' "precise locations, viewing habits, and private messages," including "data on users' phone contacts who do not themselves use TikTok." Gov't Br. 1; *see* TikTok Reply Br. 25. According to a TikTok declarant, the current version of TikTok can only "approximate users' geographic locations." Access to a user's contact list, likewise, is currently available only if a user affirmatively opts in, and it is "anonymized and used only to facilitate connections with other TikTok users." TikTok Reply Br. 25. TikTok further points to other data protections that it claims to provide, such as storing sensitive user data in the United States and controlling access to them.

The Government's data-related justification for the Act, however, does not turn on the details of TikTok's mitigation measures. Even after extended negotiations, TikTok could not satisfactorily resolve the Government's concerns. We have no doubt, and the Government has never denied, that TikTok's proposed NSA would mitigate the Government's concerns to some extent. Nor do we doubt that TikTok's voluntary mitigation efforts provide some protection. The problem for TikTok is that the Government exercised its considered judgment and concluded that mitigation efforts short of divestiture were insufficient, as a TikTok declarant puts it, to mitigate "risks to acceptable levels." At bottom, the Government lacks confidence that it has sufficient visibility and resources to monitor TikTok's promised measures, nor does it have "the requisite trust" that "ByteDance and TTUSDS would comply in good faith." The court can neither fault nor second guess the Government on these crucial points.

This situation is much like that in *Pacific Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023), which involved the Executive's decision to revoke authorizations held by PRC-controlled companies to operate communication lines in the United States. There, as here, the PRC indirectly controlled the

companies "through a web of foreign affiliates." 77 F.4th at 1163 (cleaned up). The Executive "concluded that China's ownership raised significant concerns that the [companies] would be forced to comply with Chinese government requests." *Id.* (cleaned up). The Government was concerned that the PRC could "access, monitor, store, and in some cases disrupt or misroute U.S. communications, which in turn [would] allow them to engage in espionage and other harmful activities against the United States." *Id.* (cleaned up). The Executive "further concluded that the [companies] had shown a lack of candor and trustworthiness" and therefore "nothing short of revocation would ameliorate the national-security risks." *Id.* This court declined the appellants' invitation to "second-guess" the Executive's judgment regarding the threat to national security. *Id.* at 1164. We also upheld the Executive's conclusion that the companies' "untrustworthiness would make any mitigation agreement too risky" in part because the Executive could not "comprehensively monitor compliance" or "reliably detect surreptitious, state-sponsored efforts at evasion." *Id.* at 1165–66. The same considerations similarly support the Government's judgment here.

We also reject TikTok's argument that the Government's data-related concerns are speculative. The Government "need not wait for a risk to materialize" before acting; its national security decisions often must be "based on informed judgment." *China Telecom (Ams.) Corp.*, 57 F.4th at 266. Here the Government has drawn reasonable inferences based upon the evidence it has. That evidence includes attempts by the PRC to collect data on U.S. persons by leveraging Chinese-company investments and partnerships with U.S. organizations. It also includes the recent disclosure by former TikTok employees that TikTok employees "share U.S. user data on PRC-based internal communications systems that China-based ByteDance employees can access," and that the ByteDance subsidiary

responsible for operating the platform in the United States "approved sending U.S. data to China several times." In short, the Government's concerns are well founded, not speculative.

TikTok next contends that, because other companies with operations in China collect data in the United States, its data collection is not the Government's real concern. As already explained, however, the Act complements the Data Broker Law, which limits the access of any foreign adversary country (or entity controlled by such a country) to data from third-party brokers. The Act also includes a generally applicable framework through which the Executive can address other foreign adversary controlled applications in the future. That the Act does not fully solve the data collection threat posed by the PRC does not mean it was not a step in the right direction. Moreover, TikTok does not identify any company operating a comparable platform in the United States with equivalent connections to the PRC. Nor would it be dispositive if TikTok had done so because the political branches are free to "focus on their most pressing concerns." *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 449 (2015). The Government's multi-year efforts to address the risks posed by the TikTok platform support the conclusion that TikTok was, in fact, the Government's most pressing concern.

(iii) *Content manipulation*

Preventing covert content manipulation by an adversary nation also serves a compelling governmental interest. The petitioners object for two reasons, neither of which persuades.

First, TikTok incorrectly frames the Government's justification as suppressing propaganda and misinformation. The Government's justification in fact concerns the risk of the PRC covertly manipulating content on the platform. For that reason, again, the Act is directed only at control of TikTok by

a foreign adversary nation. At points, TikTok also suggests the Government does not have a legitimate interest in countering covert content manipulation by the PRC. To the extent that is TikTok's argument, it is profoundly mistaken. "At the heart of the First Amendment lies the principle that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence. Our political system and cultural life rest upon this ideal." *Turner I*, 512 U.S. at 641. When a government — domestic or foreign — "stifles speech on account of its message . . . [it] contravenes this essential right" and may "manipulate the public debate through coercion rather than persuasion." *Id.*; *see also Nat'l Rifle Ass'n of Am.*, 602 U.S. at 187 (explaining that at the core of the First Amendment "is the recognition that viewpoint discrimination is uniquely harmful to a free and democratic society").

In this case, a foreign government threatens to distort free speech on an important medium of communication. Using its hybrid commercial strategy, the PRC has positioned itself to manipulate public discourse on TikTok in order to serve its own ends. The PRC's ability to do so is at odds with free speech fundamentals. Indeed, the First Amendment precludes a domestic government from exercising comparable control over a social media company in the United States. *See NetChoice*, 144 S. Ct. at 2407 (explaining that a state government "may not interfere with private actors' speech" because the First Amendment prevents "the government from tilting public debate in a preferred direction" (cleaned up)). Here the Congress, as the Executive proposed, acted to end the PRC's ability to control TikTok. Understood in that way, the Act actually vindicates the values that undergird the First Amendment.

Like the Supreme Court, "We also find it significant that [the Government] has been conscious of its own responsibility to consider how its actions may implicate constitutional

concerns." *Humanitarian Law Project*, 561 U.S. at 35. Rather than attempting itself to influence the content that appears on a substantial medium of communication, the Government has acted solely to prevent a foreign adversary from doing so. As our concurring colleague explains, this approach follows the Government's well-established practice of placing restrictions on foreign ownership or control where it could have national security implications. Concurring Op. 2–5; *see* 47 U.S.C. § 310(a)–(b) (restricting foreign control of radio licenses); *Pac. Networks Corp.*, 77 F.4th at 1162 (upholding the FCC's decision to revoke authorizations to operate communications lines); *Moving Phones P'ship v. FCC*, 998 F.2d 1051, 1055, 1057 (D.C. Cir. 1993) (upholding the Executive's application of the Communications Act's "ban on alien ownership" of radio licenses "to safeguard the United States from foreign influence in broadcasting" (cleaned up)); *see also Palestine Info. Off. v. Shultz*, 853 F.2d 932, 936, 945 (D.C. Cir. 1988) (upholding the Executive's divestiture order under the Foreign Missions Act regarding an organization the activities of which "were deemed inimical to America's interests"); 49 U.S.C. § 40102(a)(2), (15) (requiring that a U.S. "air carrier" be "under the actual control of citizens of the United States").

Consequently, the Act is not, as the User Petitioners suggest, an effort to "control the flow of ideas to the public." *Lamont v. Postmaster Gen.*, 381 U.S. 301, 306–07 (1965). Nor are the User Petitioners correct to characterize the TikTok-specific provisions as a prior restraint on speech or an infringement on associational rights. Were a divestiture to occur, TikTok Inc.'s new owners could circulate the same mix of content as before without running afoul of the Act. People in the United States could continue to engage with content on TikTok as at present. The only change worked by the Act is that the PRC could not "manipulate the public debate through coercion rather than persuasion." *Turner I*, 512 U.S. at 641.

TikTok resists this conclusion by emphasizing stray comments from the congressional proceedings that suggest some congresspersons were motivated by hostility to certain content. The Supreme Court, however, has repeatedly instructed that courts should "not strike down an otherwise constitutional statute on the basis of an alleged illicit legislative motive." *O'Brien*, 391 U.S. at 383; *City of Renton v. Playtime Theaters, Inc.*, 475 U.S. 41, 47–49 (1986) (rejecting speculation about the "motivating factor" behind an ordinance justified without reference to speech); *Turner I*, 512 U.S. at 652 (similar). The Act itself is the best evidence of the Congress's and the President's aim. The narrow focus of the Act on ownership by a foreign adversary and the divestiture exemption provide convincing evidence that ending foreign adversary control, not content censorship, was the Government's objective.

The petitioners nevertheless contend the divestiture provisions and an exclusion from the generally applicable track betray the Government's real purpose to ban TikTok as a means of censoring content. They claim the divestiture exemption cannot be satisfied in the time allowed by the Act, which effectively makes it a ban. Conversely, they argue an exclusion from the definition of "covered company" — for entities that operate an "application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews," § 2(g)(2)(B) — creates a loophole to the generally applicable track so large that no other company is likely ever to be subjected to the prohibitions of the Act.[10] The upshot, according to TikTok, is that the Congress

[10] The parties offer competing interpretations of this exclusion. Because we do not doubt the Government's "proffered . . . interest actually underlies the law" under either interpretation, we have no occasion to interpret that provision in this case. *Blount v. SEC*, 61 F.3d 938, 946 (D.C. Cir. 1995) (quotation omitted).

"purpose-built the Act to ban TikTok because it objects to TikTok's content." TikTok Reply Br. 28.

We discern no such motive from the divestiture provisions or the design of the generally applicable framework. Although the Government does not rebut TikTok's argument that 270 days is not enough time for TikTok to divest given its high degree of integration with ByteDance, 270 days is a substantial amount of time. If TikTok (or any company subject to the Act) is unable to divest within 270 days, it can do so later and thereby lift the prohibitions. § 2(c)(1)(A)–(B). Consequently, we detect no illicit motive on the part of the Congress to ban TikTok and suppress its speech by means of the divestiture provisions.

The same is true of the reviews exclusion, which appears to reflect a good-faith effort by the Congress to narrow the scope of the general track to applications the Congress determined to present the greatest risks to national security. That the Congress created a new mechanism by which the Executive can counter threats similar to TikTok in the future — and excluded a category of applications from that framework — does not suggest the Congress's national security concerns specific to TikTok were a charade. In fact, the Congress was not required to include a generally applicable framework at all; it could have focused only on TikTok. *See Williams-Yulee*, 575 U.S. at 452 ("The First Amendment does not put [the Congress] to [an] all-or-nothing choice"). The Congress was entitled to address the threat posed by TikTok directly and create a generally applicable framework, however imperfect, for future use. It would be inappropriate to "punish" the Congress for attempting to address future national security threats by inferring an impermissible motive. *Id.*

Second, TikTok contends the Government's content-manipulation rationale is speculative and based upon factual errors. TikTok fails, however, to grapple fully with the Government's submissions. On the one hand, the Government acknowledges that it lacks specific intelligence that shows the PRC has in the past or is now coercing TikTok into manipulating content in the United States. On the other hand, the Government is aware "that ByteDance and TikTok Global have taken action in response to PRC demands to censor content *outside* of China." The Government concludes that ByteDance and its TikTok entities "have a demonstrated history of manipulating the content on their platforms, including at the direction of the PRC." Notably, TikTok never squarely denies that it has ever manipulated content on the TikTok platform at the direction of the PRC. Its silence on this point is striking given that "the Intelligence Community's concern is grounded in the actions ByteDance and TikTok have already taken overseas." It may be that the PRC has not yet done so in the United States or, as the Government suggests, the Government's lack of evidence to that effect may simply reflect limitations on its ability to monitor TikTok.

In any event, the Government reasonably predicts that TikTok "would try to comply if the PRC asked for specific actions to be taken to manipulate content for censorship, propaganda, or other malign purposes" in the United States. That conclusion rests on more than mere speculation. It is the Government's "informed judgment" to which we give great weight in this context, even in the absence of "concrete evidence" on the likelihood of PRC-directed censorship of TikTok in the United States. *Humanitarian Law Project*, 561 U.S. at 34–35.

The purported factual errors identified by TikTok do not alter that conclusion. TikTok principally faults the Government

for claiming the recommendation engine is "based in China" because it now resides in the Oracle cloud. TikTok Reply Br. 21–22. No doubt, but the Government's characterization is nonetheless consistent with TikTok's own declarations. TikTok's declarants explained that now and under its proposed NSA "ByteDance will remain completely in control of developing the Source Code for all components that comprise 'TikTok' . . . including the Recommendation Engine." They likewise represent that TikTok presently "relies on the support of employees of other ByteDance subsidiaries" for code development. Even when TikTok's voluntary mitigation measures have been fully implemented, the "source code supporting the TikTok platform, including the recommendation engine, will continue to be developed and maintained by ByteDance subsidiary employees, including in the United States and in China." TikTok is therefore correct to say the recommendation engine "is stored in the Oracle cloud," but gains nothing by flyspecking the Government's characterization of the recommendation engine still being in China.

b. The Act is narrowly tailored.

The TikTok-specific provisions of the Act are narrowly tailored to further the Government's two national security interests. "It bears emphasis that, under the strict-scrutiny standard, a restriction must be narrowly tailored, not perfectly tailored." *In re Sealed Case*, 77 F.4th at 830–31 (cleaned up). Here the relevant provisions of the Act apply narrowly because they are limited to foreign adversary control of a substantial medium of communication and include a divestiture exemption. By structuring the Act in this way, the Congress addressed precisely the harms it seeks to counter and only those harms. Moreover, as already explained, the Act's emphasis on ownership and control follows a longstanding approach to counter foreign government control of communication media

in the United States. *E.g.*, *Pac. Networks Corp.*, 77 F.4th at 1162; *Moving Phones P'ship*, 998 F.2d at 1055–56. The petitioners argue nonetheless that there are less restrictive alternatives available and contend the Act is fatally both overinclusive and underinclusive.

(i) *TikTok's proposed NSA*

TikTok presents its proposed NSA as a less restrictive alternative. TikTok contends that, at minimum, our consideration of this alternative implicates factual disputes that require additional proceedings. TikTok, however, misapprehends the thrust of the Government's objection to the proposed NSA. A senior Executive Branch official involved in the negotiations provided several reasons for which the Executive rejected the proposal. These included lack of U.S. visibility into PRC activity, the Executive's inability to monitor compliance with the NSA, and therefore its inadequate ability to deter noncompliance; insufficient operational independence for TikTok; and insufficient data protections for Americans. Moreover, and "most fundamentally," the NSA "still permitted certain data of U.S. users to flow to China, still permitted ByteDance executives to exert leadership control and direction over TikTok's US operations, and still contemplated extensive contacts between the executives responsible for the TikTok U.S. platform and ByteDance leadership overseas." At bottom, acceptance of "the Final Proposed NSA would ultimately have relied on the Executive Branch trusting ByteDance" to comply with the agreement, which the Government understandably judged it could not do. Based upon this array of problems, the Executive rejected the proposal and pursued a legislative solution.

TikTok adamantly disagrees with the Executive's judgment. It is not, however, the job of the petitioners or of the

courts to substitute their judgments for those of the political branches on questions of national security. *See Hernández v. Mesa*, 589 U.S. 93, 113 (2020). Understandably, TikTok therefore attempts to couch its disagreement in factual terms. But TikTok does not present any truly material dispute of fact.

Consider, for example, TikTok's claim that data anonymization under TikTok's proposed NSA would effectively mitigate the Government's concerns. The Government does not dispute that TikTok's proposal provides for data anonymization; rather, it deems this protection vulnerable to circumvention and therefore insufficient to resolve the Government's data-related concerns. That is a dispute of judgment not of fact. A similar point applies to the parties' disagreement regarding the feasibility of Oracle reviewing TikTok's source code for the Government. TikTok's declarant says Oracle could apply methods consistent with industry standards to streamline that review and points out that TikTok's proposed NSA would require Oracle to conduct its initial review in 180 days. The Government does not disagree; rather, it doubts the adequacy of Oracle's review of the source code — notwithstanding "Oracle's considerable resources" — based upon extensive technical conversations with Oracle. Moreover, even after "assuming every line of Source Code could be monitored and verified," the Government still concluded that "the PRC could exert malign influence" through commercial features of the platform that would not be identified through a review of the code. TikTok's disagreement with the Government boils down to a dispute about the sufficiency of Oracle's review to mitigate threats posed by the PRC, which is a matter of judgment, not of fact.

The same is true regarding the role of TTUSDS in limiting the PRC's ability to control TikTok through ByteDance. The Government concludes that TTUSDS would be insufficiently

independent of ByteDance, fears TTUSDS could be pressured to do the latter's bidding, and doubts TTUSDS could prevent interference by ByteDance. Indeed, the Government predicts that "TTUSDS personnel here would not resist demands to comply" with directives "even if aware of pressure from the PRC government." Whether TTUSDS sufficiently mitigates the risk of PRC interference through ByteDance is ultimately an issue of judgment, not of fact.

Similarly, the parties' dispute about the adequacy of the temporary shutdown option — or "kill switch" — under the NSA centers on the Government's ultimate conclusion regarding the sufficiency of that option. The Government's declarant on this point explains that the "temporary stop would not . . . give the U.S. Government anything resembling complete discretion to shut down the TikTok platform based on its own independent assessment of national security risk and assessments from the U.S. Intelligence Community." TikTok's declarant, by contrast, characterizes the so-called "kill switch" as a "unilateral remedy" of unparalleled "magnitude in a CFIUS mitigation agreement," which could be applied by the Government if TikTok deployed unreviewed source code or if TikTok violates the protocols for handling Protected Data. Rhetoric aside, the substance of TikTok's objection is the Government's ultimate conclusion that the shutdown option would not adequately address the Government's concerns because of the limited scope of the shutdown option as well as the Government's inability to monitor TikTok.

In sum, even if we resolved every supposed factual dispute in TikTok's favor, the result would be the same. For us to conclude the proposed NSA is an equally or almost equally effective but less restrictive alternative, we would have to reject the Government's risk assessment and override its ultimate judgment. That would be wholly inappropriate after Executive

Branch officials "conducted dozens of meetings," considered "scores of drafts of proposed mitigation terms," and engaged with TikTok as well as Oracle for more than two years in an effort to work out an acceptable agreement. Here "respect for the Government's conclusions is appropriate." *Humanitarian Law Project*, 561 U.S. at 34.

The petitioners attempt to draw a distinction between the Executive's rejection of the proposed NSA and the Congress's deliberations prior to passing the Act. The petitioners complain the Congress failed even to consider TikTok's proposed NSA. Because the Act applies narrowly to the TikTok platform, TikTok goes so far as to argue the Congress was required to make legislative findings to explain its rationale for passing the Act. These objections are unavailing. The Congress "is not obligated, when enacting its statutes, to make a record of the type that an administrative agency or court does to accommodate judicial review." *Time Warner Entm't Co. v. FCC*, 93 F.3d 957, 976 (D.C. Cir. 1996) (cleaned up); *Sable Commc'ns of Cal., 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"). Moreover, the petitioners cannot credibly claim the Congress was any less aware than the Executive of the proposed NSA as a potential alternative. Prior to passage of the Act, while the Executive was negotiating the proposed NSA with TikTok, Executive Branch officials briefed congressional committees several times. The record shows that congresspersons were aware of TikTok's voluntary mitigation efforts; TikTok and its supporters, including the PRC itself, lobbied the Congress not to pass the Act; and TikTok displayed "a pop-up message urging users to contact their representatives about the Act," which prompted a deluge of calls to congresspersons. We think it clear the

Congress did not reject the proposed NSA for lack of familiarity; like the Executive, the Congress found it wanting.

To qualify as a less restrictive alternative, the proposed NSA must "accomplish the Government's goals equally or almost equally effectively." *In re Sealed Case*, 77 F.4th at 830 (cleaned up). As already stated, the Government has offered considerable evidence that the NSA would not resolve its national security concerns. Divestiture, by contrast, clearly accomplishes both goals more effectively than would the proposed NSA. It has the added virtue of doing so with greater sensitivity to First Amendment concerns by narrowly mandating an end to foreign adversary control. The proposed NSA, by contrast, contemplates an oversight role for the U.S. Government that includes what TikTok calls a "kill switch remedy" and the Government characterizes as "temporary stop" authority over the platform. Entangling the U.S. government in the daily operations of a major communications platform would raise its own set of First Amendment questions. Indeed, it could be characterized as placing U.S. government "officials astride the flow of [communications]," the very arrangement excoriated in *Lamont*, 381 U.S. at 306. Divestiture poses no such difficulty.

(ii) *Other options*

The petitioners suggest a variety of other options that the Government also found inadequate. These include disclosure or reporting requirements, the Government using speech of its own to counter any alleged foreign propaganda, limiting TikTok's collection of location and contact data, and extending the ban of TikTok on government devices to government employees' personal devices. None would "accomplish the Government's goals equally or almost equally effectively." *In re Sealed Case*, 77 F.4th at 830 (cleaned up).

The first two suggestions obviously fall short. As the Government points out, covert manipulation of content is not a type of harm that can be remedied by disclosure. 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. Moreover, the petitioners' attempt to frame the use of Government speech as a means of countering "alleged foreign propaganda," Creator Br. 54, is beside the point. It is the "secret manipulation of the content" on TikTok — not foreign propaganda — that "poses a grave threat to national security." Gov't Br. 36. No amount of Government speech can mitigate that threat nearly as effectively as divestiture.

The petitioners' other proposals are similarly flawed. Creators' contention that the Government "could simply ban TikTok from collecting . . . location and contact data" fundamentally misapprehends the Government's data-collection concerns, which are not limited to two types of data. Creator Reply Br. 29. The data-collection risks identified by the Government include the PRC's ability to use TikTok for "bulk collection of data" and for "targeted collection on individuals." Gov't Br. 48. Indeed, the FBI has specifically assessed that "TikTok could facilitate the PRC's access to U.S. users' data, which could enable PRC espionage, technology transfer, data collection and influence activities." For example, the PRC could use TikTok data to enhance its "artificial intelligence capabilities" and obtain "extensive information about users and non-users, including U.S. Government and U.S. intelligence community employees, U.S. political dissidents, and other individuals of interest to the PRC." Moreover, even if the Government's concerns were limited to certain categories of data, its inability to monitor TikTok makes a targeted prohibition on the collection of specific types of data less effective than divestiture.

For similar reasons, a limited prohibition addressing government employees would not suffice. The Government's concern extends beyond federal employees to "family members or potential future government employees (many of whom may be teenagers today, a particular problem given TikTok's popularity among young people)." Indeed, as the Government emphasizes, the Congress was legislating "in the interest of all Americans' data security." Gov't Br. 58. A more limited prohibition would not be as effective as divestiture.

The User Petitioners also identify as options various legislative proposals, such as the Adversarial Platform Prevention Act of 2021, S. 47, 117th Cong. (2021); Internet Application I.D. Act, H.R. 4000, 117th Cong. (2021); and the TELL Act, H.R. 742, 118th Cong. (2023), that the Congress did not adopt. In substance, these proposals are similar to the alternatives we just considered and found less effective than divestiture. If anything, those unenacted lesser legislative proposals undermine rather than advance the User Petitioners' preferred alternatives: That the Congress considered a series of other measures before ultimately adopting the Act implies only that the Congress determined nothing short of divestiture would sufficiently avoid the risks posed by TikTok.

In short, the petitioners suggest an array of options none of which comes close to serving either, much less both, the Government's goals as effectively as does divestiture. Each consequently fails to qualify as a less restrictive alternative for purposes of the First Amendment.

(iii) *Overinclusive / underinclusive*

The petitioners contend the Act is both overinclusive and underinclusive. They argue the Act is overinclusive primarily because the TikTok-specific provisions apply to another ByteDance product, CapCut, that can be used to edit videos on

various platforms including TikTok but does not collect user data or present an opportunity for PRC manipulation of content. Given the Government's well-supported concerns about ByteDance, it was necessary for the Act to apply to all ByteDance entities. Moreover, the petitioners fail to demonstrate that neither of the Government's two national security concerns implicate CapCut. We therefore conclude the TikTok-specific provisions of the Act are not overinclusive.

We likewise conclude the Act is not fatally underinclusive. The main purpose of inquiring into underinclusiveness is "to ensure that the proffered state interest actually underlies the law." *Nat'l Ass'n of Mfrs. v. Taylor*, 582 F.3d 1, 17 (D.C. Cir. 2009) (cleaned up). For that reason, underinclusiveness is fatal to a regulation only "if it cannot fairly be said to advance any genuinely substantial governmental interest, because it provides only ineffective or remote support for the asserted goals, or limited incremental support." *Id.* (cleaned up). As already explained, the Congress's decision separately and more immediately to address TikTok, the Executive's "most pressing" cause for concern, was permissible. *See Williams-Yulee*, 575 U.S. at 449. That would be so even if the Congress had not included the generally applicable framework to deal with other foreign adversary controlled platforms or had not passed the Data Broker Law alongside the Act. That the Government did both supports our conclusion that the Act reflects a good-faith effort on the part of the Government to address its national security concerns.

* * *

To summarize our First Amendment analysis: The Government has provided two national security justifications for the Act. We assumed without deciding the Act is subject to strict scrutiny and we now uphold the TikTok-specific portions of the Act under each justification. This conclusion is supported by ample evidence that the Act is the least restrictive means of advancing the Government's compelling national security interests.

C. Equal Protection

TikTok argues that the Act violates its right to the equal protection of the laws because it singles out TikTok for disfavored treatment relative to other similarly situated platforms. The Government contends its justifications for the Act satisfy the requirement of equal protection and add that TikTok received more process than a company would receive under the generally applicable provisions. We conclude the Act is consistent with the requirement of equal protection**.**

"In equal protection challenges the critical question is always whether there is an appropriate governmental interest suitably furthered by the differential treatment at issue." *Cmty-Serv. Broad. of Mid-Am., Inc. v. FCC*, 593 F.2d 1102, 1122 (D.C. Cir. 1978) (cleaned up). This question "lies at the intersection" of equal protection and the First Amendment. *News Am. Pub., Inc. v. FCC*, 844 F.2d 800, 804 (D.C. Cir. 1988) (cleaned up).

Although we review "conventional economic legislation" under a "minimum rationality" standard, *id.* at 802, we have held something "more is required than 'minimum rationality'" when a regulation burdens "a single publisher/broadcaster," *id.* at 814. *See also BellSouth I*, 144 F.3d at 68 (explaining that

News America does not require strict scrutiny for "statutes singling out particular persons for speech restrictions"); *Cmty-Serv. Broad. of Mid-Am., Inc.*, 593 F.2d at 1122 (applying to a "statute affecting First Amendment rights" an "equal protection standard [that] is closely related to the O'Brien First Amendment tests"). Having concluded the relevant parts of the Act do not violate the First Amendment even when subjected to heightened scrutiny, we readily reach the same conclusion when analyzing the Act in equal protection terms.

TikTok's equal protection argument boils down to pointing out that TikTok alone is singled out by name in the Act, unlike companies that in the future may be subject to the generally applicable provisions of the Act. Merely singling a company out, however, does not amount to an equal protection violation if doing so furthers an appropriate governmental interest. The controlling question is "whether there is an appropriate governmental interest suitably furthered by the differential treatment at issue." *Cmty-Serv. Broad. of Mid-Am., Inc.*, 593 F.2d at 1122–23 (holding statute violated First and Fifth Amendments by unjustifiably burdening only non-commercial broadcasters). Here the Government justified the Act by presenting two national security risks specific to the TikTok platform. By naming TikTok in the Act, the Congress ensured TikTok-related risks were addressed promptly. Simultaneously creating a generally applicable framework gave the Executive a tool to address similar risks that may come to light in the future. This differential treatment furthers the Government's national security interest in countering the immediate threat posed by the PRC's control of TikTok.

The governmental interests here also stand in stark contrast to the case upon which TikTok primarily relies, in which the "sole apparent difference" in treatment between similarly situated broadcasters was due to "an accident of timing." *News*

Am. Pub., Inc., 844 F.2d at 815. That case involved legislation that regulated waivers of the rule against newspaper-television cross-ownership in a way that targeted a single person "with the precision of a laser beam." *Id.* at 814. The legislation, however, bore "only the most strained relationship to the purpose hypothesized by the [Government]." *Id.* Here, by contrast, the Act bears directly on the TikTok-specific national security harms identified and substantiated by the Government.

Moreover, as the Government notes, in certain respects TikTok received more process than would a company coming under the generally applicable provisions. TikTok participated in a prolonged negotiation with the Executive that featured numerous meetings and several proposals. It also received individualized consideration by the Congress prior to being required to divest. In contrast, under the generally applicable provisions the Executive need only provide "public notice" and issue a "public report" to the Congress prior to requiring a company to sever its ties to an adversary nation. § 2(g)(3)(B). In short, the Act singled out TikTok because of its known characteristics and history. It therefore did not violate TikTok's constitutional right to equal protection of the laws.

D. The Bill of Attainder Clause

TikTok next claims the Act is a bill of attainder, and therefore prohibited by Article I, § 9, clause 3 of the Constitution. The Government responds that the Bill of Attainder Clause does not apply to corporations and that, in any event, the Act does not constitute a legislative punishment. We agree that the Act is not a bill of attainder.

A law is a bill of attainder if it "(1) applies with specificity, and (2) imposes punishment." *BellSouth Corp. v. FCC* (*BellSouth II*), 162 F.3d 678, 683 (D.C. Cir. 1998). Because the Act applies with specificity, this claim turns on whether the Act

can fairly be deemed a punishment. We conclude the Act is not a punishment under any of the three tests used to distinguish a permissible burden from an impermissible punishment.

Before turning to those tests, however, we briefly address the Government's threshold argument that the Bill of Attainder Clause does not apply to corporations. In other cases, we have assumed without deciding that the clause applies to corporations but emphasized that differences between commercial entities and persons need to be considered. *See, e.g.*, *Kaspersky Lab, Inc. v. DHS*, 909 F.3d 446, 453–54, 461–63 (D.C. Cir. 2018) (assuming the Bill of Attainder Clause protects corporations but emphasizing the differences between corporations and "living, breathing human beings"); *BellSouth I*, 144 F.3d at 63 & n.5 (assuming the clause protects corporations but recognizing the importance of understanding "its effect on flesh-and-blood people"). We take the same approach here.

To determine whether a law constitutes a punishment, we analyze:

> (1) whether the challenged statute falls within the historical meaning of legislative punishment [the historical test];
>
> (2) whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes [the functional test]; and
>
> (3) whether the legislative record evinces a congressional intent to punish [the motivational test].

Kaspersky Lab, Inc., 909 F.3d at 455 (cleaned up). The Act clearly is not a bill of attainder judged by any of these tests.

TikTok contends the Act satisfies the historical test because it bars TikTok from its chosen business. TikTok

reasons the prohibitions of the Act are close analogs to two categories of legislative action historically regarded as bills of attainder: confiscation of property and legislative bars to participation in a specific employment or profession. *See BellSouth II*, 162 F.3d at 685 (explaining the historical understanding of punishment). According to TikTok, the Act effectively requires TikTok to relinquish its property or see it rendered useless, and it precludes TikTok from continuing to participate in a legitimate business enterprise. As already explained, however, the Act requires a divestiture — that is, a sale, not a confiscation — as a condition of continuing to operate in the United States. *See BellSouth I*, 144 F.3d at 65 (explaining that although "structural separation is hardly costless, neither does it remotely approach the disabilities that have traditionally marked forbidden attainders"); *see also Kaspersky Lab, Inc.*, 909 F.3d at 462–63 (comparing a law requiring the Government to remove from its systems a Russia-based company's software to the business regulations in the *BellSouth* cases). Nor is the divestiture requirement analogous to a legislative bar on someone's participation in a specific employment or profession. *See Kaspersky Lab, Inc.*, 909 F.3d at 462 (rejecting a similar analogy in part "because human beings and corporate entities are so dissimilar" (cleaned up)).

The closer historical analog to the Act is a line-of-business restriction, which does not come within the historical meaning of a legislative punishment. *See BellSouth II*, 162 F.3d at 685 (observing "the Supreme Court has approved other line-of-business restrictions without ever suggesting that the restrictions constituted 'punishment'" (collecting cases)); *Kaspersky Lab, Inc.*, 909 F.3d at 463 (explaining "the *BellSouth* cases make clear that the Bill of Attainder Clause tolerates statutes that, in pursuit of legitimate goals such as public safety or economic regulation, prevent companies from engaging in particular kinds of business or particular

combinations of business endeavors"). In fact, *BellSouth II* all but forecloses TikTok's argument by recognizing that a "statute that leaves open perpetually the possibility of [overcoming a legislative restriction] does not fall within the historical meaning of forbidden legislative punishment." 162 F.3d at 685 (quoting *Selective Serv. Sys. v. Minn. Pub. Int. Rsch. Grp.*, 468 U.S. 841, 853 (1984)) (brackets in original). The qualified divestiture exemption does just that. It "leaves open perpetually" the possibility of overcoming the prohibitions in the Act: TikTok can execute a divestiture and return to the U.S. market at any time without running afoul of the law.

The Act also passes muster under the functional test. For purposes of this analysis, the "question is not whether a burden is proportionate to the objective, but rather whether the burden is so disproportionate that it belies any purported nonpunitive goals." *Kaspersky Lab, Inc.*, 909 F.3d at 455 (cleaned up). Considering our conclusion that the Act passes heightened scrutiny for purposes of the First Amendment, it obviously satisfies the functional inquiry here: The Act furthers the Government's nonpunitive objective of limiting the PRC's ability to threaten U.S. national security through data collection and covert manipulation of information. The Government's solution to those threats "has the earmarks of a rather conventional response to a security risk: remove the risk." *Id.* at 457 (cleaned up). In other words, the Government's attempt to address the risks posed by TikTok reflects a forward-looking prophylactic, not a backward-looking punitive, purpose. That is sufficient to satisfy the functional analysis. *See id.* at 460 (stating the functional test "does not require that the Congress precisely calibrate the burdens it imposes to the goals it seeks to further or to the threats it seeks to mitigate" (cleaned up)).

The so-called motivational test, for its part, hardly merits discussion. "Given the obvious restraints on the usefulness of

legislative history," congressional intent to punish is difficult to establish. *Id.* at 463 (cleaned up); *see also BellSouth II*, 162 F.3d at 690 ("Several isolated statements are not sufficient to evince punitive intent" (cleaned up)). Indeed, the motivational test is not "determinative in the absence of unmistakable evidence of punitive intent." *Id.* (cleaned up). TikTok does not come close to satisfying that requirement. We therefore conclude the Act does not violate the Bill of Attainder Clause under any of the relevant tests.

E. The Takings Clause

TikTok claims the Act constitutes a per se regulatory taking in violation of the Fifth Amendment because it will render TikTok defunct in the United States. The Government counters that TikTok has assets that can be sold, and that the Act requires only divestiture, which need not be uncompensated. Although the Act will certainly have a substantial effect on the TikTok platform in the United States, regardless whether TikTok divests, the Act does not qualify as a per se regulatory taking.

The Supreme Court recognizes two situations in which regulatory action constitutes a per se taking: (1) where the government requires that an owner suffer a "physical invasion of [its] property," and (2) where a regulation "completely deprives an owner of *all* economically beneficial use of [its] property." *Lingle v. Chevron U.S.A. Inc.*, 544 U.S. 528, 538 (2005) (cleaned up); *see Cedar Point Nursery v. Hassid*, 594 U.S. 139, 153 (2021) (explaining the first category includes temporary invasions of property). TikTok's argument is of the second variety, but it does not demonstrate the complete deprivation such a claim requires.

Here the causal connection between the Act and the alleged diminution of value is attenuated because the Act

authorizes a qualified divestiture before (or after) any prohibitions take effect. That presents TikTok with a number of possibilities short of total economic deprivation. ByteDance might spin off its global TikTok business, for instance, or it might sell a U.S. subset of the business to a qualified buyer.

TikTok dismisses divestiture as impractical. One of the main impediments, however, appears to be export prohibitions that the PRC erected to make a forced divestiture more difficult if not impossible. But the PRC, not the divestiture offramp in the Act, is the source of TikTok's difficulty. TikTok would have us turn the Takings Clause into a means by which a foreign adversary nation may render unconstitutional legislation designed to counter the national security threats presented by that very nation.

In any event, TikTok has not been subjected to a complete deprivation of economic value. Beyond characterizing divestiture as impossible, TikTok does not dispute that it 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. In other words, TikTok has several economically beneficial options notwithstanding the PRC's export restriction.

F. Alternative Relief

As an alternative to permanently enjoining the Act, the petitioners suggest we issue a temporary injunction and appoint a special master to make procedural recommendations or recommend factual findings. Because we have now resolved the case on the merits, we deny these requests as moot. The petitioners further object to the Government having filed classified material and releasing to them only a redacted version. Our decision, however, rests solely on the unredacted, public filings in this case. *See China Telecom (Ams.) Corp.*,

57 F.4th at 264 (similarly relying on an unclassified record). Notwithstanding the significant effect the Act may have on the viability of the TikTok platform, we conclude the Act is valid based upon the public record.[11]

III. Conclusion

We recognize that this decision has significant implications for TikTok and its users. Unless TikTok executes a qualified divestiture by January 19, 2025 — or the President grants a 90-day extension based upon progress towards a qualified divestiture, § 2(a)(3) — its platform will effectively be unavailable in the United States, at least for a time. Consequently, TikTok's millions of users will need to find alternative media of communication. That burden is attributable to the PRC's hybrid commercial threat to U.S. national security, not to the U.S. Government, which engaged with TikTok through a multi-year process in an effort to find an alternative solution.

The First Amendment exists to protect free speech in the United States. Here the Government acted solely to protect that freedom from a foreign adversary nation and to limit that adversary's ability to gather data on people in the United States.

For these reasons the petitions are,

Denied.

[11] Accordingly, we grant the Government's motion for leave to file classified materials and direct the Clerk to file the lodged materials, though we do not rely on them in denying the petitions.

SRINIVASAN, *Chief Judge*, concurring in part and concurring in the judgment:

I fully join all aspects of the court's opinion today other than Part II.B, which rejects TikTok's First Amendment challenge. As to that challenge, I agree with my colleagues that the Act does not violate the First Amendment. But I reach that conclusion via an alternate path. My colleagues do not decide whether the Act should be subjected to the strictest First Amendment scrutiny or instead the lesser standard of intermediate scrutiny because, in their view, the Act satisfies strict scrutiny regardless. I see no need to decide whether the Act can survive strict scrutiny, because, in my view, the Act need only satisfy intermediate scrutiny, which it does. I would thus answer the question my colleagues leave open while leaving open the question they answer.

Two features of the Act support applying intermediate rather than strict scrutiny to resolve TikTok's First Amendment challenge. First, in step with longstanding restrictions on foreign control of mass communications channels, the activity centrally addressed by the Act's divestment mandate is that of a foreign nation rather than a domestic speaker—indeed, not just a foreign nation but a designated foreign adversary. Second, the Act mandates divestment of that foreign adversary's control over TikTok for reasons lying outside the First Amendment's heartland: one reason that is wholly unrelated to speech, and another that, while connected to speech, does not target communication of any specific message, viewpoint, or content.

In those circumstances, the Act's divestment mandate need not be the least restrictive means of achieving its national-security objectives, as strict scrutiny would require. Rather, it is enough if, per intermediate scrutiny, the divestment mandate is not substantially broader than necessary to meet those goals. The Act meets that standard.

A.

TikTok's First Amendment challenge "implicates the gravest and most delicate duty that courts are called on to perform: invalidation of an Act of Congress." *Hodge v. Talkin*, 799 F.3d 1145, 1157 (D.C. Cir. 2015) (formatting modified) (quoting *Blodgett v. Holden*, 275 U.S. 142, 147–48 (1927) (Holmes, J., concurring)). And that "most delicate duty" presents itself here in a setting in which courts already proceed with suitable caution—when called upon to review the political branches' judgments about national security. A strong bipartisan majority of both Houses of Congress, together with two successive Presidents (one of whom is also the President-elect), have determined that divesting TikTok from PRC control is a national-security imperative. *See* Op., *ante*, at pp. 11–16.

While that is the political branches' across-the-board assessment of a pressing national-security issue today, we also take stock of history when considering whether their response stays within the bounds of the First Amendment. An established "history and tradition of regulation [is] relevant when considering the scope of the First Amendment." *City of Austin v. Reagan Nat'l Advert. of Austin, LLC*, 596 U.S. 61, 75 (2022) (citing *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 446 (2015)); *see Vidal v. Elster*, 602 U.S. 286, 301 (2024). It goes without saying that a social media app through which some 170 million Americans absorb information and engage with each other and the world—in the palm of their hands—is a recent phenomenon. But concerns about the prospect of foreign control over mass communications channels in the United States are of age-old vintage. In that respect, Congress's decision to condition TikTok's continued operation in the United States on severing Chinese control is not a historical outlier. Rather, it is in line with a historical pattern.

The first communications medium capable of reaching mass audiences in real time—radio—was subject to restrictions on foreign ownership and control from the very outset. The Radio Act of 1912 required radio operators engaged in interstate (or international) communications to obtain a license from the Secretary of Commerce and Labor, but Congress made licenses available only to U.S. citizens or companies. Pub. L. No. 62-264, §§ 1–2, 37 Stat. 302, 302–03 (repealed 1927). Congress then extended the restrictions to encompass foreign control (not just foreign ownership) in the Radio Act of 1927, prohibiting licensing of any company if it had a foreign officer or director or if one-fifth of its capital stock was in foreign hands. Pub. L. No. 69-632, § 12, 44 Stat. 1162, 1167 (repealed 1934).

Within a few years, the Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064, shored up the restrictions on foreign control. Section 310 of the law incorporated with little change the 1927 Act's foreign-control requirements, and also gave the newly created Federal Communications Commission (FCC) authority to withhold a license if a company is "directly or *indirectly* controlled" by a foreign-dominated parent company. *Id*. § 310(a), 48 Stat. at 1086 (emphasis added) (today codified at 47 U.S.C. § 310(b)(4) (2024)). In urging Congress to adopt the additional restrictions on foreign control, the Navy conveyed its concerns that foreign-controlled stations could "be employed in espionage work and in the dissemination of subversive propaganda." Hearings on H.R. 8301 Before the H. Comm. on Interstate & Foreign Com., 73d Cong. 26 (1934). The FCC has described Section 310's original purpose as "protect[ing] the integrity of ship-to-shore and governmental communications" from foreign interference and "thwart[ing] the airing of foreign propaganda on broadcast stations." Foreign Investment in Broadcast Licenses, 78 Fed. Reg. 75563, 75564 (Nov. 13, 2013).

Section 310 continues to restrict foreign control of radio licenses, including ones used for broadcast communication and wireless cellular services. *See* 47 U.S.C. § 310(a)–(b). And while that provision regulates wireless licenses, limitations on foreign control also exist for *wired* transmission lines under Section 214 of the same law. 47 U.S.C. § 214(a); *see also id.* § 153(11), (50)–(53).

When deciding whether to issue or revoke a Section 214 authorization, the FCC considers "the public convenience and necessity," *id.* § 214(c), including the implications for "national defense," *id.* § 151. In conducting that inquiry, the FCC assesses whether direct or indirect foreign ownership or control of a transmission line raises national-security or foreign-policy concerns. *See Rules & Policies on Foreign Participation in the U.S. Telecomm. Mkt.*, 12 FCC Rcd. 23891, 23918–21 (1997). The FCC consults with Executive Branch agencies "to help assess national security and other concerns that might arise from a carrier's foreign ownership." *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 261 (D.C. Cir. 2022). Those "Executive Branch agencies may review existing authorizations for national-security risks and recommend revocation if the risks cannot be mitigated." *Id.* at 262.

Notably, the FCC in recent years has exercised its Section 214 authority to deny or revoke transmission authorizations in the case of U.S. entities subject to ultimate Chinese control. The Commission's rationale has mirrored Congress's motivation for the Act we consider in this case—i.e., national-security concerns that the PRC could leverage its control over foreign parent companies to require U.S. subsidiaries to provide China with access to U.S. communications lines, thereby enabling espionage and other harmful undertakings. *See Pac. Networks Corp. & ComNet (USA) LLC*, 37 FCC Rcd. 4220 (2022); *China Telecom (Americas) Corp.*, 36 FCC Rcd.

15966 (2021); *China Mobile Int'l (USA)*, 34 FCC Rcd. 3361 (2019). This court has affirmed those FCC decisions. *See Pac. Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023); *China Telecom*, 57 F.4th 256.

China Telecom, for example, involved a U.S. company with a Section 214 authorization whose parent corporation was majority-owned by a Chinese governmental entity. *See* 57 F.4th at 260, 265. The FCC's revocation of China Telecom's authorization was "grounded [in] its conclusion that China Telecom poses an unacceptable security risk" because "the Chinese government is able to exert significant influence over [it]." *Id.* at 265. In rejecting China Telecom's claim that the asserted national-security risk was unduly speculative, we noted that Chinese law obligates Chinese companies "to cooperate with state-directed cybersecurity supervision and inspection," and we cited "compelling evidence that the Chinese government may use Chinese information technology firms as vectors of espionage and sabotage." *Id.* at 265–66. We additionally explained that "[i]n the national security context," the FCC "need not wait for a risk to materialize before revoking a section 214 authorization." *Id.* at 266.

China Telecom is a present-day application of the kinds of restrictions on foreign control that have existed in the communications arena since the dawn of radio. That longstanding regulatory history bears on the First Amendment analysis here. *See City of Austin*, 596 U.S. at 75. That is so even though some of that history arose in the context of broadcast, a medium in which the Supreme Court has "recognized special justifications for regulation." *Reno v. Am. Civ. Liberties Union*, 521 U.S. 844, 868 (1997). Some of the relevant history also arose outside of broadcast (e.g., authorizations for wired transmission lines under Section 214), and certain regulatory concerns are present to a far greater

degree with modern communications media than with traditional broadcast (e.g., the vastly enhanced potential for collection of data from and about users).

To be sure, because communications media reaching mass audiences in real time "were not present in the founding era," the regulatory history naturally does not date back that far. *See City of Austin*, 596 U.S. at 75. But under the Supreme Court's decisions, regulatory history still matters so long as the relevant kind of "regulation followed" on the heels of the emergence of a new type of communication medium. *Id*. In fact, it can matter for precisely the issue considered here: whether a First Amendment challenge should be examined under strict or intermediate scrutiny.

So, in *City of Austin*, the Supreme Court recently assessed which of those standards should govern a challenge to a law attaching different restrictions to off-premises and on-premises signage. *See id.* at 67–69. The Court explained that comparable regulations emerged relatively soon after outdoor billboards first appeared in the 1800s. *See id.* at 65–66, 75. To the Court, that "unbroken tradition of on-/off-premises distinctions counsel[ed] against" subjecting the challenged law to strict scrutiny. *Id.* at 75. If so there, so too here.

B.

In *City of Austin*, the Supreme Court considered the longstanding regulatory history as part of its inquiry into whether the law in question should be deemed content based or content neutral. *See* 596 U.S. at 69–76. That distinction in turn informs the standard of scrutiny. Under hornbook First Amendment doctrine, content-based laws generally pose more pronounced First Amendment concerns and so usually must satisfy strict scrutiny. *See Reed v. Town of Gilbert*, 576 U.S. 155, 163–64 (2015); *cf. City of Austin*, 596 U.S. at 73 (noting

that regulation of commercial speech has been subject to intermediate scrutiny even when content based). Content-neutral laws, on the other hand, present less substantial First Amendment concerns and so generally trigger, at most, intermediate scrutiny. *See Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994) (*Turner I*).

There can also be, though, an antecedent question: whether the First Amendment applies at all. The question arises here because the effect of the Act's divestment mandate falls most directly on foreign entities: the Act targets the PRC, a foreign sovereign, and the divestment mechanism established by Congress necessarily encompasses ByteDance, a foreign company subject to the PRC's control. That recognition brings into play the settled understanding that "foreign organizations operating abroad have no First Amendment rights." *Agency for Int'l Dev. v. All. for Open Soc'y Int'l Inc.*, 591 U.S. 430, 436 (2020).

The Act requires TikTok to divest the corporate parent, ByteDance, because ByteDance is subject to the PRC's control. ByteDance developed and maintains the source code underlying TikTok's recommendation engine, *see* Simkins Decl. ¶¶ 52, 57, 90 (TikTok App. 738, 740, 751); Presser Decl. ¶¶ 63–64 (TikTok App. 832), so the company has the ability to curate the content sent to TikTok users. That kind of curation function, when the First Amendment applies, is protected expressive activity. As the Supreme Court recently explained, "presenting a curated compilation of speech originally created by others" via a social media app is a form of expression. *Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2400 (2024); *see id.* at 2400–02. So, by forcing ByteDance to split from TikTok, the Act abolishes the ability of ByteDance—and ultimately the PRC, Congress's true concern—to curate content going to TikTok's U.S. users.

To the extent the PRC or ByteDance might wish to adjust the content viewed by U.S. users of TikTok, those curation decisions would be made abroad. *See* Milch Decl. ¶ 29 (TikTok App. 661) (explaining that TikTok's proposed security measures contemplate "continued reliance on ByteDance engineers for . . . its recommendation engine"). The PRC and ByteDance thus would lack any First Amendment rights in connection with any such curation actions. *Agency for Int'l Dev.*, 591 U.S. at 436. That is true even though the PRC or ByteDance, in that scenario, would aim their curation decisions at the United States. The Supreme Court's decision in *Agency for International Development* demonstrates the point.

That case involved foreign organizations' speech that was targeted in part at the United States, yet the Court still applied the rule that the foreign speakers lack any First Amendment rights when engaged in expressive activity abroad. The federal statute challenged in *Agency for International Development* required organizations receiving certain U.S. aid dollars to espouse a policy opposing prostitution. *Id.* at 432. The Court first held that the compelled adoption of an anti-prostitution viewpoint violated the First Amendment as applied to U.S. funding recipients. *See Agency for Int'l Dev. v. All. for Open Soc'y Int'l Inc.*, 570 U.S. 205, 214 (2013). But the Court later rejected a parallel challenge brought by foreign funding recipients, reasoning that foreign organizations lack any First Amendment rights in connection with their expressive activities abroad. *Agency for Int'l Dev.*, 591 U.S. at 433–36. And that was so even though the relevant speech act—the mandated expression of opposition to prostitution—was aimed in part at the United States: in fact, the way the funding recipients demonstrated adherence to the funding condition was to express opposition to prostitution in the "award

documents" exchanged with the U.S. Agency for International Development. *See Agency for Int'l Dev*, 570 U.S. at 210.

In short, while the Act's divestment mandate directly affects—and aims to eliminate—the ability of the PRC and ByteDance to engage with U.S. users of a PRC-controlled TikTok, it raises no First Amendment concerns vis-à-vis those foreign actors.

C.

Even if ByteDance and the PRC lack First Amendment rights to assert against the Act's divestment mandate, what about the U.S.-based petitioners' free-speech claims? The principal U.S. petitioners are: (i) TikTok Inc., the U.S. subsidiary of ByteDance that provides the TikTok platform in the United States; and (ii) U.S. TikTok users, who are both creators and viewers of TikTok content.

1.

For TikTok Inc., the Act is designed to sever ByteDance from the platform but leave untouched TikTok Inc.'s expression on a post-divestment version of the app. TikTok Inc. both creates and curates content on the platform, and the Act does not restrict those speech and curation choices. TikTok Inc. posts videos to its own TikTok account and would remain fully free to continue doing so post-divestment. The company can also engage in content moderation, including through enforcement of community guidelines that excise videos containing nudity, for instance. *See* Op., *ante*, at p. 27. To the extent those choices are TikTok Inc.'s own, the company could maintain the same editorial policies on a post-divestment version of the app.

TikTok also claims that TikTok Inc.'s deployment of the platform's recommendation engine in the U.S. is itself an expressive decision. Even assuming so, after divestment, a non-Chinese-controlled TikTok could still use the same algorithm to promote the same exact mix of content presently appearing on the app. According to TikTok, however, Chinese law would prevent the export of the algorithm fueling the recommendation engine without the PRC's approval, which it would not grant. TikTok Br. 24. The *Act*, though, would not dictate that outcome. Rather, the PRC, backed by Chinese law, would. And Congress of course need not legislate around another country's preferences to exercise its own powers constitutionally—much less the preferences of a designated foreign adversary, the very adversary whom Congress determined poses the fundamental threat to national security prompting the Act in the first place.

2.

The last group of petitioners bringing a First Amendment claim are users who create and consume content on the TikTok platform. They face the prospect of the app becoming unavailable to them if a divestment does not occur within the window allowed by Congress, or of an app potentially altered in certain ways if a divestment were to take place.

A threshold question bearing significantly on the assessment of their First Amendment challenge is which standard of scrutiny should apply: strict or intermediate scrutiny. The choice can be an important, potentially outcome-determinative one, which is why the Supreme Court can devote entire decisions to the issue. *See, e.g.*, *City of Austin*, 596 U.S. 61. That choice here, as is often the case, turns in significant measure on the rationale for the challenged law, which informs whether the law is considered content based or content neutral.

As my colleagues explain, the Act's divestment mandate rests on two justifications, both of which concern the PRC's ability (through its control over ByteDance) to exploit the TikTok platform in ways inimical to U.S. national security. *See* Op., ante, at p. 33. First, the PRC could harvest abundant amounts of information about the 170 million U.S. app users and potentially even their contacts. Second, the PRC could direct the TikTok platform to covertly manipulate the content flowing to U.S. users. To the government, a foreign adversary's ability to acquire sensitive information on Americans and secretly shape the content fed to Americans would pose a substantial threat to U.S. national security.

Those dual interests are manifested in the terms of the Act, in its central provisions establishing the divestment requirement. The Act defines a "qualified divestiture" as one that removes any ongoing relationship with the foreign adversary-controlled entities with which the app was previously affiliated, including in particular "any cooperation with respect to *the operation of a content recommendation algorithm* or an agreement with respect to *data sharing*." § 2(g)(6)(B) (emphasis added). In the central operative provision of the Act, then, Congress established that a divestiture must satisfy the two national-security concerns invoked by the government in this case: data protection and content manipulation.

An examination of those interests, separately and in combination, shows that the Act does not raise the kinds of core free-speech concerns warranting the application of strict scrutiny. Instead, intermediate scrutiny should apply.

a.

The data-protection rationale is plainly content neutral, supporting the application of intermediate rather than strict scrutiny. There is no sense in which the data-protection interest relates to the content of speech appearing on TikTok. In fact, the interest does not relate to speech at all, raising the question whether it would even trigger intermediate scrutiny if it stood alone.

In *Arcara v. Cloud Books, Inc.*, 478 U.S. 697 (1986), for instance, the Supreme Court considered a First Amendment challenge to the proposed closure of a bookstore because prostitution took place there. The Court declined to apply even intermediate scrutiny. The Court explained that, while the First Amendment claim arose from the establishment's engagement in the protected activity of selling books, that activity had nothing to do with the reasons for the proposed closure. *See id.* at 705. The Court analogized the circumstances to ones in which a "city impose[s] closure penalties for demonstrated Fire Code violations or health hazards from inadequate sewage treatment." *Id.* In such a situation, "the First Amendment would not aid the owner of premises who had knowingly allowed such violations to persist." *Id.*

Here, similarly, the data-protection rationale has nothing to do with the expressive activity taking place on the TikTok platform. Any enterprise collecting vast amounts of data from users, whatever its line of business, could pose that sort of risk. That is not to diminish the burdens on millions of U.S. users if the TikTok platform were to become unavailable to them as a forum for expressive activity. All of them could be faced with needing to find an alternate venue. The same was true, though, of the bookstore patrons in *Arcara*, yet the Court still denied

the First Amendment challenge to the bookstore's closure without even applying intermediate scrutiny.

To be sure, the *Arcara* Court observed that First Amendment scrutiny would apply to a law that "inevitably single[s] out bookstores or others engaged in First Amendment protected activities for the imposition of its burden." *Id.* Even if that description has salience here—which is not at all clear—the Court has explained that such a law may be "justified by some special characteristic" of the regulated entities. *Minneapolis Star v. Minn. Comm'r of Rev.*, 460 U.S. 575, 585 (1983); *Turner I*, 512 U.S. at 660–61. The vast data-collection practices of TikTok and similar applications subject to the Act would seem to qualify as just such a "special characteristic."

At any rate, there is no need to reach a firm conclusion on whether the data-protection interest, if considered in isolation, would trigger the application of intermediate scrutiny or instead an even more relaxed form of review. That is because the government makes no argument that the Act's application to TikTok should be sustained based on the data-protection interest alone. It is necessary, then, to engage with the other interest underpinning the Act, to which I turn next.

b.

Congress's interest in preventing the PRC's use of TikTok to engage in covert content manipulation is self-evidently connected to speech: it centers on the potential reactions of American viewers to covert content-curation decisions made by the PRC. Still, that interest does not raise heartland First Amendment concerns about content-based restrictions for reasons I will explain—so much so that, even if that interest were the sole rationale for the Act, there would still be a strong argument for applying intermediate rather than strict scrutiny.

It is important to keep in mind, though, that Congress's covert-content-manipulation concern does not stand alone. There is also its distinct data-protection interest that supports applying (at most) intermediate scrutiny, along with the consistent regulatory history of restricting foreign control of mass communications channels that likewise weighs in favor of intermediate scrutiny. So, the question ultimately is not whether the covert-content-manipulation concern itself would occasion applying strict scrutiny, but rather whether it so strongly and clearly does that it overcomes the other important considerations counseling *against* strict scrutiny. I believe it does not.

First, even assuming the covert-content-manipulation concern may bear the indicia of a content-based rationale, it would do so only marginally. The Supreme Court has used slightly varying formulations when describing what makes a law content based, but this recent articulation captures the gist: not just "*any* examination of speech or expression inherently" makes a regulation content based; rather, "it is regulations that discriminate based on 'the topic discussed or the idea or message expressed' that are content based." *City of Austin*, 596 U.S. at 73–74 (quoting *Reed*, 576 U.S. at 171); *see* Op., *ante*, at p. 28.

Congress's concern about the PRC's capacity to conduct covert content manipulation on the TikTok platform does not "discriminate based on the topic discussed or the idea or message expressed." *City of Austin*, 596 U.S. at 73–74 (internal quotation marks omitted). Congress desires to prevent the PRC's secret curation of content flowing to U.S. users *regardless* of the topic, idea, or message conveyed. *See* Gov't Br. 66–68. To be sure, Congress would have concerns about the PRC covertly compelling ByteDance to flood the feeds of American users with pro-China propaganda. But

Congress would also have concerns about the PRC sowing discord in the United States by promoting videos—perhaps even primarily truthful ones—about a hot-button issue having nothing to do with China. Indeed, because the concern is with the PRC's manipulation of the app to advance China's *interests*—not China's views—one can imagine situations in which it would even serve the PRC's interests to augment *anti*-China, *pro*-U.S. content. Suppose, for instance, the PRC determines that it is in its interest to stir an impression of elevated anti-China sentiment coming from the United States—say, to conjure a justification for actions China would like to take against the United States. That would qualify as covert content manipulation of the kind that concerned Congress and supports the Act's divestment mandate.

Congress's concern with covert content manipulation by a foreign adversary in any direction and on any topic—rather than on particular messages, subjects, or views—is evident in the Act's terms and design. *See City of Renton v. Playtime Theaters, Inc.*, 475 U.S. 41, 48 (1986); *Turner I*, 512 U.S. at 646–49, 652. Recall that the Act asks whether there is the prospect of "any cooperation" with an entity controlled by a foreign adversary "with respect to the operation of a content recommendation algorithm." § 2(g)(6)(B). The concern is a general one about control of a "content recommendation algorithm," without regard to whether the content choices enabled by that control might point in a specific direction or involve a specific matter.

As is reflected in the title of the Act—"Protecting Americans From Foreign Adversary Controlled Applications Act"—Congress aimed not to address specific content but to address specific actors: in particular, to prevent a "foreign adversary" from exercising control over covered applications. In that sense, the law operates in the nature of a speaker-based

restriction. As applied here, what matters is whether a particular potential curator, the PRC, has the ability to control (covertly) the content fed to TikTok's U.S. users, regardless of what the content may be. True, "laws favoring some speakers over others demand strict scrutiny" when the "speaker preference reflects a content preference." *Reed*, 576 U.S. at 171 (quoting *Turner I*, 512 U.S. at 658). But here, the speaker (non)preference is not grounded in a content preference.

In certain respects, in fact, the Act resembles a time, place, or manner regulation—a type of regulation generally subject to intermediate scrutiny. *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984); *Ward v. Rock Against Racism*, 491 U.S. 781, 791, 798–99 (1989). The Act restricts only one way in which the Chinese government can project information into the United States—the covert manipulation of content on TikTok. The Act does not touch on the PRC's ability to communicate through any medium other than TikTok (and potentially other "covered" applications, *see* § 2(g)(2)(A)). Indeed, as far as the Act is concerned, the PRC would be free to publish its own videos—whether labeled as such or camouflaged as cutout accounts—on a post-divestment version of *TikTok itself*. So understood, the Act does not prevent Americans from receiving any message from the PRC; it only prevents the PRC from secretly manipulating the content on a specific channel of communication that it ultimately controls.

Those circumstances are far removed from *Lamont v. Postmaster General*, 381 U.S. 301 (1965), on which petitioners heavily rely. *Lamont* concerned a law requiring anyone in the United States who desired to receive mail deemed by the Secretary of the Treasury to be "communist political propaganda" to affirmatively notify the Postal Service. *Id.* at 302–03. The Supreme Court invalidated the statute, resting its

decision "on the narrow ground that the addressee in order to receive his mail must request in writing that it be delivered." *Id.* at 307. That obligation amounted to "an unconstitutional abridgement of the addressee's First Amendment rights," because "any addressee is likely to feel some inhibition in sending for literature which federal officials have condemned as 'communist political propaganda.'" *Id.*

This case does not involve the "narrow ground" on which the Court rooted its decision in *Lamont*: an affirmative obligation to out oneself to the government in order to receive communications from a foreign country that are otherwise permitted to be here. Moreover, whereas this case, as explained, addresses what amounts to a speaker-based regulation without a content preference underpinning it, the law in *Lamont* drew a viewpoint-based distinction based on whether the government deemed mailed material "communist political propaganda." Finally, *Lamont* was not a case about *covert* content manipulation, the concern driving the Act's divestment mandate. In that regard, while counterspeech is an available response in the case of a publication designated as "communist political propaganda," counterspeech is elusive in response to covert (and thus presumably undetected) manipulation of a social media platform.

* * *

For all those reasons, Congress's concern with the PRC's potential exercise of covert content manipulation should not give rise to strict scrutiny. That concern does not bear the hallmarks of a content-based rationale; the Act's other justification concerning data protection is plainly a content-neutral one; and there has been a long regulatory history of restrictions on foreign control of mass communications channels.

D.

To satisfy intermediate scrutiny, a law needs to meet two requirements: (i) the law must further "important" (or "substantial" or "legitimate") governmental interests; and (ii) the means must be narrowly tailored to serve those interests. *See Turner I*, 512 U.S. at 661–62; *Ward*, 491 U.S. at 791, 796, 798–99. Under strict scrutiny, by comparison: (i) the governmental interests must be "compelling"; and (ii) the means must be the least-restrictive way of serving them. *E.g.*, *McCullen v. Coakley*, 573 U.S. 464, 478 (2014). As to the second prong, the Supreme Court has explained that the "narrow tailoring" test under intermediate scrutiny requires less than the least-restrictive-means test under strict scrutiny, with the former met "[s]o long as the means chosen are not substantially broader than necessary to achieve the government's interest." *Ward*, 491 U.S. at 800.

Here, the Act satisfies both prongs of the intermediate scrutiny test.

1.

Recall that, as manifested in the Act's terms and design, *see* § 2(g)(6)(B), Congress mandated TikTok's divestment in order to prevent the PRC from capturing the personal data of millions of Americans and surreptitiously manipulating the content the app serves them. Each of those objectives qualifies as an important governmental interest.

a.

The data-protection interest aims to protect U.S. national security by depriving the PRC of access to a vast dataset of granular information on 170 million Americans. Congress's interest is important and well grounded.

As TikTok does not dispute, the platform collects vast amounts of information from and about its American users. *See* TikTok App. 820; Privacy Policy, TikTok (Aug. 28, 2024), https://perma.cc/XE6G-F86Q. The government's national-security concerns about the PRC's access to that data take two forms. First, the PRC could exploit sensitive data on individual Americans to undermine U.S. interests, including by recruiting assets, identifying Americans involved in intelligence, and pressuring and blackmailing our citizens to assist China. Second, the vast information about Americans collected by TikTok amounts to the type of "bulk" dataset that could "greatly enhance" China's development and use of "artificial intelligence capabilities." Vorndran Decl. ¶ 32 (Gov't App. 37).

Those national-security concerns self-evidently qualify as important. To be sure, the fears must be "real, not merely conjectural." *Turner I*, 512 U.S. at 664. And petitioners submit that the government's concerns about the PRC accessing user data from the TikTok platform are unduly speculative and insufficiently grounded. I cannot agree.

When applying intermediate scrutiny, a court "must accord substantial deference to the predictive judgments of Congress," and "[o]ur sole obligation is to assure that, in formulating its judgments, Congress has drawn reasonable inferences based on substantial evidence." *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 195 (1997) (*Turner II*) (internal quotation marks omitted). That bar is cleared here.

In evaluating whether Congress's national-security concerns are adequately grounded, we can take stock of the Executive Branch's elaborations as submitted in declarations. *See Humanitarian Law Project*, 561 U.S. at 33. As my colleagues set out, Op., *ante*, at pp. 34–36, and as the

government explains, Congress's data-security concern arises against a backdrop of broadscale "overt and covert actions" by the PRC "to undermine U.S. interests," Blackburn Decl. ¶ 23 (Gov't App. 8). Collecting data on Americans is a key part of that multi-faceted strategy. *See id.* ¶¶ 31–33 (Gov't App. 10–11). The PRC has engaged in extensive efforts to amass data on Americans for potential use against U.S. interests. *Id.* ¶ 31 (Gov't App. 10–11). And the PRC "is rapidly expanding and improving its artificial intelligence and data analytics capabilities for intelligence purposes," enabling it to exploit access to large datasets in increasingly concerning ways. *Id.* ¶ 30 (Gov't App. 10).

"ByteDance and TikTok present powerful platforms" for those purposes. *Id.* ¶ 36 (Gov't App. 13). It is a modus operandi of the PRC to surreptitiously access data through its control over companies like ByteDance. While the PRC has sometimes obtained data through aggressive hacking operations, it also attempts to do so by "leverag[ing] access through its relationships with Chinese companies." *Id.* ¶ 33 (Gov't App. 11). Even if the PRC has yet to discernibly act on its potential control over ByteDance's access to data on American users in particular, Congress did not need to wait for the risk to become realized and the damage to be done before taking action to avert it. *See Humanitarian Law Project*, 561 U.S. at 34–35; *China Telecom*, 57 F.4th at 266–67. That is particularly so in light of the PRC's broader, long-term geopolitical strategy of pre-positioning assets for potential use against U.S. interests at pivotal moments. *See* Vorndran Decl. ¶ 12 (Gov't App. 34); Blackburn Decl. ¶ 26 (Gov't App. 9).

In these circumstances, in short, Congress's data-protection concern is hardly speculative or inadequately grounded in this murky corner of national security.

b.

The same is true of Congress's concern about the PRC's covert content manipulation. Our duty to accord deference to Congress's determinations when applying intermediate scrutiny, *Turner II*, 520 U.S. at 195, is all the more important in the area of national security. Like its data-protection concern, Congress's content-manipulation concern "arise[s] in connection with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess." *Humanitarian Law Project*, 561 U.S. at 34. In matters of national security, Congress must often rely on its—and the Executive Branch's—"informed judgment rather than concrete evidence." *Id.* at 34–35. And "[t]hat reality affects what we may reasonably insist on from the Government." *Id.* at 35. The government's "evaluation of the facts" is "entitled to deference." *Id.* at 33.

As the government details and petitioners do not dispute, the PRC engages in an aggressive, global campaign of influence operations against U.S. interests, relying heavily on the internet and social-media platforms. Blackburn Decl. ¶¶ 28–29 (Gov't App. 9–10). Across the globe, the PRC seeks to "promote PRC narratives . . . and counter other countries' policies that threaten the PRC's interests." *Id.* ¶ 29 (Gov't App. 10). That includes increasingly pronounced efforts to "mold" America's "public discourse" and "magnify" our "societal divisions." *Id.*

It was reasonable for Congress to infer from the information available to it that, if directed by the PRC to assist in those efforts, ByteDance and TikTok "would try to comply." *Id.* ¶ 69 (Gov't App. 23). The government points to examples of when "the PRC has exerted control over the content shown on other ByteDance-managed apps." Vorndran Decl. ¶ 33

(Gov't App. 38). And were the PRC to exert that kind of covert control over the content on TikTok, it would be "difficult—if not impossible—to detect, both by TikTok users and by law enforcement personnel." *Id.* ¶ 34 (Gov't App. 38). In that context, Congress's concern with preventing the PRC's covert content manipulation of the platform readily qualifies as an important, well-founded governmental interest.

In resisting that conclusion, petitioners contend that the covert-content-manipulation rationale cannot be an important governmental interest because it is "related to the suppression of free expression." *NetChoice*, 144 S. Ct. at 2407. Petitioners are mistaken.

As an initial matter, insofar as petitioners believe that a law can *never* satisfy First Amendment scrutiny if it is "related to the suppression of free expression," that is incorrect. The consequence of a law's being deemed "related to the suppression of expression" is not that the law is then per se invalid, but instead that it is then subject to strict rather than intermediate scrutiny. *See Humanitarian Law Project*, 561 U.S. at 28 (citing *Texas v. Johnson*, 491 U.S. 397, 403 (1989)). In this case, for all the reasons previously explained, the Act's divestment mandate is more appropriately assessed under intermediate scrutiny than strict scrutiny.

That conclusion is fully consistent with *NetChoice*, as the laws at issue there were "related to the suppression of expression" in a way untrue of the Act. In *NetChoice*, two states enacted laws addressing perceived bias against conservative viewpoints on large social-media platforms like YouTube and Facebook. 144 S. Ct. at 2394. The laws restricted the platforms' ability to remove, label, or deprioritize posts or users based on content or viewpoint. *Id.* at 2395–96. The laws did so, the Supreme Court explained, in pursuit of an

objective "to correct the mix of speech that the major social-media platforms present," so as "to advance [the states'] own vision of ideological balance." *Id.* at 2407. The Court explained that such an interest "is very much related to the suppression of free expression, and it is not valid, let alone substantial." *Id.* (citing *Buckley v. Valeo*, 424 U.S. 1, 48–49 (1976) (per curiam)).

Here, by contrast, the Act is not grounded in any congressional aim to correct a perceived viewpoint imbalance on the TikTok platform by achieving a different ideological mix. Congress, as discussed, did not seek to prevent covert content manipulation by the PRC in furtherance of any overarching objective of suppressing (or elevating) certain viewpoints, messages, or content. *Supra* pp. 14–16. Instead, Congress's objective was to protect our national security from the clandestine influence operations of a designated foreign adversary, regardless of the possible implications for the mix of views that may appear on the platform.

While that alone sets this case apart from *NetChoice*, *see* 144 S. Ct. at 2408 n.10, it also bears emphasis that the laws at issue in *NetChoice* did not serve a distinct interest entirely unrelated to the suppression of free expression. Here, on the other hand, the Act rests in significant measure on Congress's data-protection interest, an interest indisputably having no relation to the suppression of speech. For that reason as well, *NetChoice* poses no obstacle to concluding that the Act serves important governmental interests for purposes of intermediate scrutiny.

2.

The Act's divestment mandate is narrowly tailored to achieve Congress's important national-security interests in preventing the PRC from accessing U.S. TikTok users' data

and covertly manipulating content on the platform. The Act will bring about the severing of PRC control of the TikTok platform in the United States, either through a divestment of that control, or, if no qualifying divestment takes place, through a prohibition on hosting or distributing a still-PRC-controlled TikTok in the United States until a qualifying divestment occurs. The divestment mandate is "not substantially broader than necessary to achieve" Congress's national-security objectives. *Ward*, 491 U.S. at 800.

Congress confined the Act to applications subject to the control of just four designated foreign adversary countries, including China. § 2(g)(4); *see* 10 U.S.C. § 4872(d)(2). As applied here, the divestment mandate is fashioned to permit the TikTok platform—including its recommendation engine—to continue operating in the United States. *Supra* p. 10. Insofar as the PRC's (or ByteDance's) own decisions may prevent that from happening, the independent decisions of those foreign actors cannot render Congress's chosen means substantially overbroad.

TikTok submits that various alternate means—including its proposed National Security Agreement (NSA), *see* Op., *ante*, at pp. 13–15—would equally fulfill Congress's aims without giving rise to the prospect of the platform's suspended operations in the United States. But even if we thought that were true, it would not help TikTok under intermediate scrutiny: under that standard, "[s]o long as the means chosen are not substantially broader than necessary," a law "will not be invalid simply because a court concludes that the government's interest could be adequately served by some less-speech-restrictive alternative." *Ward*, 491 U.S. at 800; *see Turner II*, 520 U.S. at 217–18. A court instead must "defer to [Congress's] reasonable determination" of how "its interest[s] . . . would be best served." *Ward*, 491 U.S. at 800.

Here, Congress reasonably determined that attaining the requisite degree of protection required mandating a divestment of PRC control. A "disagreement over the level of protection . . . to be afforded and how protection is to be attained" does not constitute a basis for "displac[ing] Congress' judgment" when applying intermediate scrutiny. *Turner II*, 520 U.S. at 224. And Congress's resolution here is in line with other situations in which national-security concerns can call for divestment of a foreign country's control over a U.S. company. *See* 50 U.S.C. § 4565(d)(1); H.R. Rep. No. 118-417, at 5–6 & n.26.

Nor could TikTok succeed under intermediate scrutiny by pointing to evidence that, in its view, contradicts Congress's determination that nothing shy of divestment would be sufficient. TikTok argues, for instance, that in concluding the NSA was an inadequate alternative, the government misunderstood certain aspects of its design and operation—e.g., how difficult it would be to review TikTok's source code. "[R]egardless of whether the evidence is in conflict" on such matters, a court can still sustain a challenged law when applying intermediate scrutiny. *Turner II*, 520 U.S. at 211. That is because "the relevant inquiry" under that standard is "not whether Congress, as an objective matter, was correct to determine [its chosen means are] necessary" to meet its objectives. *Id.*; *see id.* at 196. "Rather, the question is whether the legislative conclusion was reasonable and *supported by substantial evidence in the record before Congress*." *Id.* at 211 (emphasis added). It was here.

The Executive Branch believed, and specifically advised Congress, that measures short of divestment would not adequately protect against the risks to national security posed by the PRC's potential control of the TikTok platform. *See* Newman Decl. ¶ 7 (Gov't App. 47); Redacted Hearing Tr. 11–

14. With specific regard to the provisions contained in the proposed NSA, "senior Executive Branch officials concluded that the terms of ByteDance's final proposal would not sufficiently ameliorate those risks." Newman Decl. ¶ 6 (Gov't App. 46). The provisions, in the Executive Branch's view, "still permitted certain data of U.S. users to flow to China, still permitted ByteDance executives to exert leadership control and direction over TikTok's US operations, and still contemplated extensive contacts between the executives responsible for the TikTok U.S. platform and ByteDance leadership overseas." *Id.* ¶ 75 (Gov't App. 62). And, the Executive Branch assessed, the NSA "would have ultimately relied on . . . trusting ByteDance" to comply, but "the requisite trust did not exist." *Id.* ¶¶ 75, 86 (Gov't App. 62, 68).

Those concerns about the kinds of provisions in the NSA and the overarching lack of trust were discussed with Congress. *See* Redacted Hearing Tr. 10–12, 40–42, 49–50. Congress's reliance on those Executive Branch conclusions, even if they are now disputed by TikTok, means its "legislative conclusion was . . . supported by substantial evidence in the record before [it]." *Turner II*, 520 U.S. at 211; *see id.* at 198–99 (relying on conflicted testimony before Congress).

* * * * *

While the court today decides that the Act's divestment mandate survives a First Amendment challenge, that is not without regard for the significant interests at stake on all sides. Some 170 million Americans use TikTok to create and view all sorts of free expression and engage with one another and the world. 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.

To give effect to those competing interests, Congress chose divestment as a means of paring away the PRC's control—and thus containing the security threat—while maintaining the app and its algorithm for American users. But if no qualifying divestment occurs—including because of the PRC's or ByteDance's unwillingness—many Americans may lose access to an outlet for expression, a source of community, and even a means of income.

Congress judged it necessary to assume that risk given the grave national-security threats it perceived. And because the record reflects that Congress's decision was considered, consistent with longstanding regulatory practice, and devoid of an institutional aim to suppress particular messages or ideas, we are not in a position to set it aside.