Per Curiam:

As of January 19, the Protecting Americans from Foreign Adversary Controlled Applications Act will make it unlawful for companies in the United States to provide services to distribute, maintain, or update the social media platform TikTok, unless U.S. operation of the platform is severed from Chinese control. Petitioners are two TikTok operating entities and a group of U.S. TikTok users. We consider whether the Act, as applied to petitioners, violates the First Amendment.

In doing so, we are conscious that the cases before us involve new technologies with transformative capabilities. This challenging new context counsels caution on our part. As Justice Frankfurter advised 80 years ago in considering the application of established legal rules to the "totally new problems" raised by the airplane and radio, we should take care not to "embarrass the future." *Northwest Airlines, Inc.* v. *Minnesota*, 322 U.S. 292, 300 (1944). That caution is heightened in these cases, given the expedited time allowed for our consideration.[1] Our analysis must be understood to be narrowly focused in light of these circumstances.

I

A

TikTok is a social media platform that allows users to create, publish, view, share, and interact with short videos overlaid with audio and text. Since its launch in 2017, the platform has accumulated over 170 million users in the United States and more than one billion worldwide. Those users are prolific content creators and viewers. In 2023, U.S. TikTok users uploaded more than 5.5 billion videos, which were in turn viewed more than 13 trillion times around the world.

Opening the TikTok application brings a user to the "For You" page—a personalized content feed tailored to the user's interests. TikTok generates the feed using a proprietary algorithm that recommends videos to a user based on the user's interactions with the platform. Each interaction a user has on TikTok—watching a video, following an account, leaving a comment—enables the recommendation system to further tailor a personalized content feed.

A TikTok user's content feed is also shaped by content moderation and filtering decisions. TikTok uses automated and human processes to remove content that violates the platform's community guidelines. TikTok also promotes or demotes certain content to advance its business objectives and other goals. TikTok is operated in the United States by TikTok Inc., an American company incorporated and headquartered in California. TikTok Inc.'s ultimate parent company is ByteDance Ltd., a privately held company that has operations in China. ByteDance Ltd. owns TikTok's proprietary algorithm, which is developed and maintained in China. The company is also responsible for developing portions of the source code that runs the TikTok platform. ByteDance Ltd. is subject to Chinese laws that require it to "assist or cooperate" with the Chinese Government's "intelligence work" and to ensure that the Chinese Government has "the power to access and control private data" the company holds. H. R. Rep. No. 118–417, p. 4 (2024) (H. R. Rep.).

---

1 Applications for an injunction pending review were filed on December 16, 2024; we construed the applications as petitions for a writ of certiorari and granted them on December 18, 2024; and oral argument was held on January 10, 2025.

B

1

In recent years, U.S. government officials have taken repeated actions to address national security concerns regarding the relationship between China and TikTok. In August 2020, President Trump issued an Executive Order finding that "the spread in the United States of mobile applications developed and owned by companies in [China] continues to threaten the national security, foreign policy, and economy of the United States." Exec. Order No. 13942, 3 C.F.R. 412 (2021). President Trump determined that TikTok raised particular concerns, noting that the platform "automatically captures vast swaths of information from its users" and is susceptible to being used to further the interests of the Chinese Government. *Id.* The President invoked his authority under the International Emergency Economic Powers Act (IEEPA), 50 U.S. C. § 1701 *et seq*., and the National Emergencies Act, 50 U.S. C. § 1601 *et seq*., to prohibit certain "transactions" involving ByteDance Ltd. or its subsidiaries, as identified by the Secretary of Commerce. 3 C.F.R. 413. ... But federal courts enjoined the prohibitions before they took effect, finding that they exceeded the Executive Branch's authority under IEEPA. See generally *TikTok Inc.* v. *Trump*, 507 F. Supp. 3d 92 (D.D.C. 2020); *Marland* v. *Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020). Just days after issuing his initial Executive Order, President Trump ordered ByteDance Ltd. to divest all interests and rights in any property "used to enable or support ByteDance's operation of the TikTok application in the United States," along with "any data obtained or derived from" U.S. TikTok users. 85 Fed. Reg. 51297. ByteDance Ltd. and TikTok Inc. filed suit in the D. C. Circuit, challenging the constitutionality of the order. In February 2021, the D. C. Circuit placed the case in abeyance to permit the Biden administration to review the matter and to enable the parties to negotiate a non-divestiture remedy that would address the Government's national security concerns. Throughout 2021 and 2022, ByteDance Ltd. negotiated with Executive Branch officials to develop a national security agreement that would resolve those concerns. Executive Branch officials ultimately determined, however, that ByteDance Ltd.'s proposed agreement did not adequately mitigate the risks posed to U.S. national security interests. Negotiations stalled, and the parties never finalized an agreement.

2

Against this backdrop, Congress enacted the Protecting Americans from Foreign Adversary Controlled Applications Act. Pub. L. 118–50, div. H, 138 Stat. 955. The Act makes it unlawful for any entity to provide certain services to "distribute, maintain, or update" a "foreign adversary controlled application" in the United States. § 2(a)(1). Entities that violate this prohibition are subject to civil enforcement actions and hefty monetary penalties. See §§ 2(d)(1)(A), (d)(2)(B).

The Act provides two means by which an application may be designated a "foreign adversary controlled application." First, the Act expressly designates any application that is "operated, directly or indirectly," by "ByteDance Ltd." or "TikTok," or any subsidiary or successor thereof. § 2(g)(3)(A). Second, the Act establishes a general designation framework for any application that is both (1) operated by a "covered company" that is "controlled by a foreign adversary," and (2) "determined by the President to present a significant threat to the national security of the United States," following a public notice and reporting process. § 2(g)(3)(B). In broad terms, the Act defines "covered company" to include a company that operates an application that enables users to generate, share, and view content and has more

than 1,000,000 monthly active users. § 2(g)(2)(A). The Act excludes from that definition a company that operates an application "whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." § 2(g)(2)(B).

The Act's prohibitions take effect 270 days after an application is designated a foreign adversary controlled application. § 2(a)(2). Because the Act itself designates applications operated by "ByteDance, Ltd." and "TikTok," prohibitions as to those applications take effect 270 days after the Act's enactment—January 19, 2025. The Act exempts a foreign adversary controlled application from the prohibitions if the application undergoes a "qualified divestiture." § 2(c)(1). A "qualified divestiture" is one that the President determines will result in the application "no longer being controlled by a foreign adversary." § 2(g)(6)(A). The President must further determine that the divestiture "precludes the establishment or maintenance of any operational relationship between the United States operations of the [application] and any formerly affiliated entities that are controlled by a foreign adversary, including any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing." § 2(g)(6)(B). The Act permits the President to grant a one-time extension of no more than 90 days with respect to the prohibitions' 270-day effective date if the President makes certain certifications to Congress regarding progress toward a qualified divestiture. § 2(a)(3).

C

ByteDance Ltd. and TikTok Inc.—along with two sets of TikTok users and creators (creator petitioners)—filed petitions for review in the D.C. Circuit, challenging the constitutionality of the Act. As relevant here, the petitioners argued that the Act's prohibitions, TikTok-specific foreign adversary controlled application designation, and divestiture requirement violate the First Amendment. …

II

A

At the threshold, we consider whether the challenged provisions are subject to First Amendment scrutiny. Laws that directly regulate expressive conduct can, but do not necessarily, trigger such review. We have also applied First Amendment scrutiny in cases involving governmental regulation of conduct that has an expressive element, and to some statutes which, although directed at activity with no expressive component, impose a disproportionate burden upon those engaged in protected First Amendment activities.

It is not clear that the Act itself directly regulates protected expressive activity, or conduct with an expressive component. Indeed, the Act does not regulate the creator petitioners at all. And it directly regulates ByteDance Ltd. and TikTok Inc. only through the divestiture requirement. See § 2(c)(1). Petitioners, for their part, have not identified any case in which this Court has treated a regulation of corporate control as a *direct* regulation of expressive activity or semi-expressive conduct. We hesitate to break that new ground in this unique case.

In any event, petitioners' arguments more closely approximate a claim that the Act's prohibitions, TikTok-specific designation, and divestiture requirement impose a disproportionate burden upon their First Amendment activities. Petitioners assert—and the Government does not contest—that, because it is commercially infeasible for TikTok to be divested within the Act's 270-day timeframe, the Act effectively bans TikTok in the United States. Petitioners argue that such a ban will

burden various First Amendment activities, including content moderation, content generation, access to a distinct medium for expression, association with another speaker or preferred editor, and receipt of information and ideas.

We have recognized a number of these asserted First Amendment interests. See *Moody* v. *NetChoice, LLC*, 603 U.S. 707, 731 (2024) ("An entity exercising editorial discretion in the selection and presentation of content is engaged in speech activity."); *City of Ladue* v. *Gilleo*, 512 U.S. 43, 54–58 (1994) ("Our prior decisions have voiced particular concern with laws that foreclose an entire medium of expression."); *Rumsfeld* v. *Forum for Academic and Institutional Rights, Inc.*, 547 U.S. 47, 68 (2006) ("We have recognized a First Amendment right to associate for the purpose of speaking, which we have termed a 'right of expressive association.'"); *Martin* v. *City of Struthers*, 319 U.S. 141, 143 (1943) ("The right of freedom of speech and press ... embraces the right to distribute literature and necessarily protects the right to receive it.").[2] And an effective ban on a social media platform with 170 million U.S. users certainly burdens those users' expressive activity in a non-trivial way.

At the same time, a law targeting a foreign adversary's control over a communications platform is in many ways different in kind from the regulations of non-expressive activity that we have subjected to First Amendment scrutiny. Those differences—the Act's focus on a foreign government, the congressionally determined adversary relationship between that foreign government and the United States, and the causal steps between the regulations and the alleged burden on protected speech—may impact whether First Amendment scrutiny applies.

This Court has not articulated a clear framework for determining whether a regulation of non-expressive activity that disproportionately burdens those engaged in expressive activity triggers heightened review. We need not do so here. We assume without deciding that the challenged provisions fall within this category and are subject to First Amendment scrutiny.

B

***1*...**

We have identified two forms of content-based speech regulation. First, a law is content based on its face if it applies to particular speech because of the topic discussed or the idea or message expressed. Second, a facially content-neutral law is nonetheless treated as a content-based regulation of speech if it cannot be justified without reference to the content of the regulated speech or was adopted by the government because of disagreement with the message the speech conveys.

As applied to petitioners, the challenged provisions are facially content neutral and are justified by a content-neutral rationale.

a

The challenged provisions are facially content neutral. They impose TikTok-specific prohibitions due to a foreign adversary's control over the platform and make divestiture a prerequisite for the platform's continued operation in the United States. They do not target particular speech based upon its content, contrast, *e.g.*, *Carey* v. *Brown*, 447 U.S. 455, 465 (1980) (statute prohibiting all residential pick-

---

2 To the extent that ByteDance Ltd.'s asserted expressive activity occurs abroad, that activity is not protected by the First Amendment. See *Agency for Int'l Development* v. *Alliance for Open Society Int'l Inc.*, 591 U.S. 430, 436 (2020) ("Foreign organizations operating abroad have no First Amendment rights.").

eting except "peaceful labor picketing"), or regulate speech based on its function or purpose, contrast, *e.g.*, *Holder* v. *Humanitarian Law Project*, 561 U.S. 1, 7, 27 (2010) (law prohibiting providing material support to terrorists). Nor do they impose a "restriction, penalty, or burden" by reason of content on TikTok—a conclusion confirmed by the fact that petitioners cannot avoid or mitigate the effects of the Act by altering their speech. As to petitioners, the Act thus does not facially regulate "particular speech because of the topic discussed or the idea or message expressed." *Reed*, 576 U.S., at 163. Petitioners argue that the Act is content based on its face because it excludes from the definition of "covered company" any company that operates an application "whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." § 2(g)(2)(B). We need not decide whether that exclusion is content based. The question before the Court is whether the Act violates the First Amendment *as applied to petitioners*. To answer that question, we look to the provisions of the Act that give rise to the effective TikTok ban that petitioners argue burdens their First Amendment rights. The exclusion for certain review platforms, however, applies only to the general framework for designating applications controlled by "covered companies," not to the TikTok-specific designation. §§ 2(g)(3)(A)–(B). As such, the exclusion is not within the scope of petitioners' as-applied challenge.

b

The Government also supports the challenged provisions with a content-neutral justification: preventing China from collecting vast amounts of sensitive data from 170 million U.S. TikTok users. That rationale is decidedly content agnostic. It neither references the content of speech on TikTok nor reflects disagreement with the message such speech conveys. *Cf. Ward*, 491 U.S., at 792–793 (holding noise control and sound quality justifications behind city sound amplification guideline were content neutral). Because the data collection justification reflects a "purpose unrelated to the content of expression," it is content neutral. *Id.*, at 791.

2

The Act's TikTok-specific distinctions, moreover, do not trigger strict scrutiny. It is true that "speech restrictions based on the identity of the speaker are all too often simply a means to control content." *Citizens United* v. *Federal Election Comm'n*, 558 U.S. 310, 340 (2010). For that reason, "regulations 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. But while "laws favoring some speakers over others demand strict scrutiny when the legislature's speaker preference reflects a content preference," *id.*, at 658, such scrutiny "is unwarranted when the differential treatment is justified by some special characteristic of the particular speaker being regulated," *id.*, at 660–661.

For the reasons we have explained, requiring divestiture for the purpose of preventing a foreign adversary from accessing the sensitive data of 170 million U.S. TikTok users is not "a subtle means of exercising a content preference." *Turner I*, 512 U.S., at 645. The prohibitions, TikTok-specific designation, and divestiture requirement regulate TikTok based on a content-neutral data collection interest. And TikTok has special characteristics—a foreign adversary's ability to leverage its control over the platform to collect vast amounts of personal data from 170 million U.S. users—that justify this differential treatment. "Speaker distinctions of this nature are not presumed invalid under the First Amendment." *Id.*

While we find that differential treatment was justified here, however, we emphasize the inherent narrowness of our holding. Data collection and analysis is a common practice in this digital age. But TikTok's scale and susceptibility to foreign adversary control, together with the vast swaths of sensitive data the platform collects, justify differential treatment to address the Government's national security concerns. A law targeting any other speaker would by necessity entail a distinct inquiry and separate considerations.

On this understanding, we cannot accept petitioners' call for strict scrutiny. No more than intermediate scrutiny is in order.

C

As applied to petitioners, the Act satisfies intermediate scrutiny. The challenged provisions further an important Government interest unrelated to the suppression of free expression and do not burden substantially more speech than necessary to further that interest.[3]

1

The Act's prohibitions and divestiture requirement are designed to prevent China—a designated foreign adversary—from leveraging its control over ByteDance Ltd. to capture the personal data of U.S. TikTok users. This objective qualifies as an important Government interest under intermediate scrutiny.

Petitioners do not dispute that the Government has an important and well-grounded interest in preventing China from collecting the personal data of tens of millions of U.S. TikTok users. Nor could they. The platform collects extensive personal information from and about its users. See H. R. Rep., at 3 (Public reporting has suggested that TikTok's "data collection practices extend to age, phone number, precise location, internet address, device used, phone contacts, social network connections, the content of private messages sent through the application, and videos watched."); 1 App. 241 (Draft National Security Agreement noting that TikTok collects user data, user content, behavioral data (including "keystroke patterns and rhythms"), and device and network data (including device contacts and calendars)). If, for example, a user allows TikTok access to the user's phone contact list to connect with others on the platform, TikTok can access "any data stored in the user's contact list," including names, contact information, contact photos, job titles, and notes. 2 *id.*, at 659. Access to such detailed information about U.S. users, the Government worries, may enable "China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." 3 C.F.R. 412. And Chinese law enables China to require companies to surrender data to the government, "making companies headquartered there an espionage tool" of China. H. R. Rep., at 4.

Rather than meaningfully dispute the scope of the data TikTok collects or the ends to which it may be used, petitioners contest probability, asserting that it is "unlikely" that China would "compel TikTok to turn over user data for intelligence-gathering purposes, since China has more effective and efficient means of obtaining relevant information." In reviewing the constitutionality of the Act, however, we must accord substantial deference to the predictive judgments of Congress. Sound policymaking often requires legislators to forecast future events and to anticipate the likely impact of these events based on deductions and inferences for

---

3 Our holding and analysis are based on the public record, without reference to the classified evidence the Government filed below.

which complete empirical support may be unavailable. Here, the Government's TikTok-related data collection concerns do not exist in isolation. The record reflects that China "has engaged in extensive and yearslong efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations." 2 App. 634.

Even if China has not yet leveraged its relationship with ByteDance Ltd. to access U.S. TikTok users' data, petitioners offer no basis for concluding that the Government's determination that China might do so is not at least a reasonable inference based on substantial evidence. We are mindful that this law arises in a context in which "national security and foreign policy concerns arise 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. We thus afford the Government's informed judgment substantial respect here.

Petitioners further argue that the Act is underinclusive as to the Government's data protection concern, raising doubts as to whether the Government is actually pursuing that interest. In particular, petitioners argue that the Act's focus on applications with user-generated and user-shared content, along with its exclusion for certain review platforms, exempts from regulation applications that are "as capable as TikTok of collecting Americans' data." But the First Amendment imposes no freestanding underinclusiveness limitation, and the Government need not address all aspects of a problem in one fell swoop. Furthermore, as we have already concluded, the Government had good reason to single out TikTok for special treatment. Contrast *Brown* v. *Entertainment Merchants Assn.*, 564 U.S. 786, 802 (2011) (singling out purveyors of video games for disfavored treatment without a persuasive reason "raised serious doubts about whether the government was in fact pursuing the interest it invoked, rather than disfavoring a particular speaker or viewpoint"). On this record, Congress was justified in specifically addressing its TikTok-related national security concerns.

2

As applied to petitioners, the Act is sufficiently tailored to address the Government's interest in preventing a foreign adversary from collecting vast swaths of sensitive data about the 170 million U.S. persons who use TikTok. To survive intermediate scrutiny, a regulation need not be the least speech-restrictive means of advancing the Government's interests. Rather, the standard "is satisfied so long as the regulation promotes a substantial government interest that would be achieved less effectively absent the regulation" and does not "burden substantially more speech than is necessary" to further that interest. *Ward*, 491 U.S., at 799. The challenged provisions meet this standard. The provisions clearly serve the Government's data collection interest "in a direct and effective way." *Ward*, 491 U.S., at 800. The prohibitions account for the fact that, absent a qualified divestiture, TikTok's very operation in the United States implicates the Government's data collection concerns, while the requirements that make a divestiture "qualified" ensure that those concerns are addressed before TikTok resumes U.S. operations. Neither the prohibitions nor the divestiture requirement, moreover, is substantially broader than necessary to achieve this national security objective. Rather than ban TikTok outright, the Act imposes a conditional ban. The prohibitions prevent China from gathering data from U.S. TikTok users unless and until a qualified divestiture severs China's control.

Petitioners parade a series of alternatives—disclosure requirements, data sharing restrictions, the proposed national security agreement, the general designation provision—that they assert would address the Government's data collection interest in equal measure to a conditional TikTok ban. Those alternatives do not alter our tailoring analysis.

Petitioners' proposed alternatives ignore the latitude we afford the Government to design regulatory solutions to address content-neutral interests. "So long as the means chosen are not substantially broader than necessary to achieve the government's interest, ... the regulation 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. For the reasons we have explained, the challenged provisions are not substantially broader than necessary to address the Government's data collection concerns. Nor did the Government ignore less restrictive approaches already proven effective. The validity of the challenged provisions does not turn on whether we agree with the Government's conclusion that its chosen regulatory path is best or"most appropriate. "We cannot displace [the Government's] judgment respecting content-neutral regulations with our own, so long as its policy is grounded on reasonable factual findings supported by evidence that is substantial for a legislative determination." *Turner II*, 520 U.S., at 224. Those requirements are met here.

D

In addition to the data collection concerns addressed above, the Government asserts an interest in preventing a foreign adversary from having control over the recommendation algorithm that runs a widely used U.S. communications platform, and from being able to wield that control to alter the content on the platform in an undetectable manner. In petitioners' view, that rationale is a content-based justification that "taints" the Government's data collection interest and triggers strict scrutiny. ...

Petitioners have not pointed to any case in which this Court has assessed the appropriate level of First Amendment scrutiny for an Act of Congress justified on both content-neutral and content-based grounds. They assert, however, that the challenged provisions are subject to—and fail—strict scrutiny because Congress would not have passed the provisions absent the foreign adversary control rationale. We need not determine the proper standard for mixed-justification cases or decide whether the Government's foreign adversary control justification is content neutral. Even assuming that rationale turns on content, petitioners' argument fails under the counterfactual analysis they propose: The record before us adequately supports the conclusion that Congress would have passed the challenged provisions based on the data collection justification alone.

To start, the House Report focuses overwhelmingly on the Government's data collection concerns, noting the "breadth" of TikTok's data collection, "the difficulty in assessing precisely which categories of data" the platform collects, the "tight interlinkages" between TikTok and the Chinese Government, and the Chinese Government's ability to "coerce" companies in China to "provide data." H. R. Rep., at 3; see *id*., at 5–12 (recounting a five-year record of Government actions raising and attempting to address those very concerns). Indeed, it does not appear that any legislator disputed the national security risks associated with TikTok's data collection practices, and nothing in the legislative record suggests that data collection was anything but an overriding congressional concern. We are especially wary of parsing Congress's motives on this record with regard to an Act passed with

striking bipartisan support. See 170 Cong. Rec. H1170 (Mar. 13, 2024) (352–65); 170 Cong. Rec. S2992 (Apr. 23, 2024) (79–18). Petitioners assert that the text of the Act itself undermines this conclusion. In particular, they argue that the Government's data collection rationale cannot justify the requirement that a qualified divestiture preclude "any operational relationship" that allows for "cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing." § 2(g)(6)(B). We disagree. The Government has explained that ByteDance Ltd. uses the data it collects to train the TikTok recommendation algorithm, which is developed and maintained in China. According to the Government, ByteDance Ltd. has previously declined to agree to stop collecting U.S. user data or sending that data to China to train the algorithm. The Government has further noted the difficulties associated with monitoring data sharing between ByteDance Ltd. and TikTok Inc. Under these circumstances, we find the Government's data collection justification sufficient to sustain the challenged provisions.

* * *

There is no doubt that, for more than 170 million Americans, TikTok offers a distinctive and expansive outlet for expression, means of engagement, and source of community. But Congress has determined that divestiture is necessary to address its well-supported national security concerns regarding TikTok's data collection practices and relationship with a foreign adversary. For the foregoing reasons, we conclude that the challenged provisions do not violate petitioners' First Amendment rights. ...

Justice Sotomayor, concurring in part and concurring in the judgment:

I join all but Part II.A of the Court's *per curiam* opinion. I see no reason to assume without deciding that the Act implicates the First Amendment because our precedent leaves no doubt that it does.

TikTok engages in expressive activity by "compiling and curating" material on its platform. *Moody* v. *NetChoice, LLC*, 603 U.S. 707, 731 (2024). Laws that impose a disproportionate burden upon those engaged in expressive activity are subject to heightened scrutiny under the First Amendment. The challenged Act plainly imposes such a burden: It bars any entity from distributing TikTok's speech in the United States, unless TikTok undergoes a qualified divestiture.

The Act, moreover, effectively prohibits TikTok from collaborating with certain entities regarding its "content recommendation algorithm" even following a qualified divestiture. § 2(g)(6)(B). And the Act implicates content creators' "right to associate" with their preferred publisher "for the purpose of speaking." *Rumsfeld* v. *Forum for Academic and Institutional Rights, Inc.*, 547 U.S. 47, 68 (2006). That, too, calls for First Amendment scrutiny.

As to the remainder of the *per curiam* opinion, I agree that the Act survives petitioners' First Amendment challenge.

Justice Gorsuch, concurring in judgment.

We have had a fortnight to resolve, finally and on the merits, a major First Amendment dispute affecting more than 170 million Americans. Briefing finished on January 3, argument took place on January 10, and our opinions issue on January 17, 2025. Given those conditions, I can sketch out only a few, and admittedly tentative, observations.

First, the Court rightly refrains from endorsing the government's asserted interest in preventing "the covert manipulation of content" as a justification for the

law before us. One man's "covert content manipulation" is another's "editorial discretion." Journalists, publishers, and speakers of all kinds routinely make less-than-transparent judgments about what stories to tell and how to tell them. Without question, the First Amendment has much to say about the right to make those choices. It makes no difference that Americans (like TikTok Inc. and many of its users) may wish to make decisions about what they say in concert with a foreign adversary. "Those who won our independence" knew the vital importance of the "freedom to think as you will and to speak as you think," as well as the dangers that come with repressing the free flow of ideas. *Whitney* v. *California*, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring). ...

Second, I am pleased that the Court declines to consider the classified evidence the government has submitted to us but shielded from petitioners and their counsel. Efforts to inject secret evidence into judicial proceedings present obvious constitutional concerns. ...

Third, I harbor serious reservations about whether the law before us is content neutral and thus escapes strict scrutiny. More than that, while I do not doubt that the various "tiers of scrutiny" discussed in our case law— "rational basis, strict scrutiny, something(s) in between"— can help focus our analysis, I worry that litigation over them can sometimes take on a life of its own and do more to obscure than to clarify the ultimate constitutional questions.

Fourth, whatever the appropriate tier of scrutiny, I am persuaded that the law before us seeks to serve a compelling interest: preventing a foreign country, designated by Congress and the President as an adversary of our Nation, from harvesting vast troves of personal information about tens of millions of Americans. The record before us establishes that TikTok mines data both from TikTok users and about millions of others who do not consent to share their information. 2 App. 659. According to the Federal Bureau of Investigation, TikTok can access "*any data*" stored in a consenting user's "contact list"—including names, photos, and other personal information about unconsenting third parties. *Id.* (emphasis added). And because the record shows that the People's Republic of China (PRC) can require TikTok's parent company "to cooperate with its efforts to obtain personal data," there is little to stop all that information from ending up in the hands of a designated foreign adversary. *Id.*, at 696. The PRC may then use that information to "build dossiers ... for blackmail," "conduct corporate espionage," or advance intelligence operations. 1 App. 215. To be sure, assessing exactly what a foreign adversary may do in the future implicates "delicate" and "complex" judgments about foreign affairs and requires "large elements of prophecy." *Chicago & Southern Air Lines, Inc.* v. *Waterman S. S. Corp.*, 333 U.S. 103, 111 (1948) (Jackson, J., for the Court). But the record the government has amassed in these cases after years of study supplies compelling reason for concern.

Finally, the law before us also appears appropriately tailored to the problem it seeks to address. Without doubt, the remedy Congress and the President chose here is dramatic. The law may require TikTok's parent company to divest or (effectively) shutter its U.S. operations. But before seeking to impose that remedy, the coordinate branches spent years in negotiations with TikTok exploring alternatives and ultimately found them wanting. And from what I can glean from the record, that judgment was well founded. Consider some of the alternatives. Start with our usual and preferred remedy under the First Amendment: more speech. However helpful that might be, the record shows that warning users of the risks associated with giving their data to a foreign-adversary-controlled application would do

nothing to protect nonusers' data. Forbidding TikTok's domestic operations from sending sensitive data abroad might seem another option. But even if Congress were to impose serious criminal penalties on domestic TikTok employees who violate a data-sharing ban, the record suggests that would do little to deter the PRC from exploiting TikTok to steal Americans' data. See 1 App. 214 (noting threats from "malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development" in the PRC); 2 App. 702 ("Agents of the PRC would not fear monetary or criminal penalties in the United States"). The record also indicates that the size and complexity of TikTok's underlying software may make it impossible for law enforcement to detect violations. Even setting all these challenges aside, any new compliance regime could raise separate constitutional concerns—for instance, by requiring the government to surveil Americans' data to ensure that it isn't illicitly flowing overseas.

Whether this law will succeed in achieving its ends, I do not know. A determined foreign adversary may just seek to replace one lost surveillance application with another. As time passes and threats evolve, less dramatic and more effective solutions may emerge. Even what might happen next to TikTok remains unclear. But the question we face today is not the law's wisdom, only its constitutionality. Given just a handful of days after oral argument to issue an opinion, I cannot profess the kind of certainty I would like to have about the arguments and record before us. All I can say is that, at this time and under these constraints, the problem appears real and the response to it not unconstitutional. As persuaded as I am of the wisdom of Justice Brandeis in *Whitney* and Justice Holmes in *Abrams*, their cases are not ours. Speaking with and in favor of a foreign adversary is one thing. Allowing a foreign adversary to spy on Americans is another.