Per Curiam

SUPREME COURT OF THE UNITED STATES

Nos. 24–656 and 24–657

TIKTOK INC., ET AL., PETITIONERS
24–656
MERRICK B. GARLAND, ATTORNEY GENTw 7.o4.9 (NTw 7.u.4 (GE)-4.9 (NT-)-4 Pe

care not to "embarrass the future."
v. , 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

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.); see 2 App. 673–676.

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 CFR 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. The President invoked his authority under the International Emergency Economic Powers Act (IEEPA), 50 U. S. C. §1701 ., and the National Emergencies Act, 50 U. S. C. §1601 ., to prohibit certain "transactions" involving ByteDance Ltd. or its subsidiaries, as identified by the Secretary of Commerce. 3 CFR 413. The Secretary published a list of prohibited transactions in September 2020. See 85

U. S. ___ (2024).

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. See v. , 505 U. S. 377, 382–386 (1992). We have also applied First Amendment scrutiny in "cases involving governmental reg-

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

"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." v. , 512 U. S. 622, 641 (1994) ( ). Government action that suppresses speech because of its message "contravenes this essential right." "Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." v. , 576 U. S. 155, 163 (2015). Content-neutral laws, in contrast, "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." , 512 U. S., at 642 (citation omitted). Under that standard, we will sustain a content-neutral law "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." v. , 520 U. S. 180, 189 (1997) ( ).

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." , 576 U. S., at 163; see , at 163–164 (explaining that some facial distinctions define regulated speech by subject matter, others by the speech's function or purpose). 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.'" ., at 164 (quoting v. , 491 U. S. 781, 791 (1989)).

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, . ., v. , 447 U. S. 455, 465 (1980) (statute prohibiting all residential picketing except "peaceful labor picketing"), or regulate speech based on its function or purpose, contrast, . ., v. , 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. , 512 U. S., at 644. As to petitioners, the Act thus does not facially regulate "particular speech because of the topic discussed or the idea or message expressed." , 576 U. S., at 163.

Petitioners argue that the Act is content based on its face

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, behav-

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 ., 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 CFR 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 anl -03 1 6 h-7 0 Td calen18 turIn-7 viewf8y(to)-5.4hsers4 (uT3 Dantesute th

ers offer no basis for concluding that the Government's determination that China might do so is not at least a "reasonable inferenc[e] based on substantial evidence."
, 520 U. S., at 195. 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."
, 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-geartsg(0 0 alarf -.adp1ren9p)62 ƀBDC 0.00.ren31o60 0 1

Per Curiam

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."

Petitioners' proposed alternatives ignore the "latitude" we afford the Government to design regulatory solutions to address content-neutral interests. , 520 U. S., at 213. "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 alterna-

i

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. See 2 App. 628. In petitioners' view, that rationale is a content-based justification that "taint[s]" the Government's data collection interest and triggers strict scrutiny. Brief for TikTok 41.

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. See Brief for TikTok 41–42; Brief for Creator Petitioners 47–50. 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 "coerc[e]" companies in China to "provid[e] data." H. R. Rep., at 3; see ., 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

SUPREME COURT OF THE UNITED STATES

Nos. 24–656 and 24–657

TIKTOK INC., ET AL., PETITIONERS
24–656
MERRICK B. GARLAND, ATTORNEY GENERAL

BRIAN FIREBAUGH, ET AL., PETITIONERS
24–657
MERRICK B. GARLAND, ATTORNEY GENERAL

ON APPLICATIONS FOR INJUNCTION PENDING REVIEW TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 17, 2025]

JUSTICE SOTOMAYOR, concurring in part and concurring in the judgment.

I join all but Part II.A of the Court's 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. v. , 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. v. ., 478 U. S. 697, 704 (1986); see

orating with certain entities regarding its "content recommendation algorithm" even following a qualified divestiture. §2(g)(6)(B), 138 Stat. 959. And the Act implicates content creators' "right to associate" with their preferred publisher "for the purpose of speaking." v. ., 547 U. S. 47, 68 (2006). That, too, calls for First Amendment scrutiny.

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

GORSUCH,

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. v. , 274 U. S. 357, 375 (1927) (Brandeis, J., concurring). They knew, too, that except in the most extreme situations, "the fitting remedy for evil counsels is good ones." . Too often in recent years, the

24–657, pp. 8–11. 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. v. , 742 F. 3d 922, 932 (CA10 2014) (Gorsuch, J., concurring).

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 " " stored in a consenting user's "contact list"—including names, photos, and other personal information about unconsenting third parties. (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. , at 696; see , at 673–676; at 3. The PRC may then use that information to "build dossiers . . . for blackmail," "conduct corporate espionage," or advance intelligence operations. 1 App. 215; see 2 App. 659. 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." v. , 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

"direct U. S. government monitoring" of the "flow of U. S. user data").

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. See Tr. of Oral Arg. 146–147. 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 and Justice Holmes in , their cases are not ours. See , at 2. Speaking with and in favor of a foreign adversary is one thing. Allowing a foreign adversary to spy on Americans is another.