Nos. 24-656, 24-657

IN THE
Supreme Court of the United States

TIKTOK, INC., ET AL.,
Petitioners,
V.

MERRICK B. GARLAND, ATTORNEY GENERAL,
Respondent.

BRIAN FIREBAUGH, ET AL.,
Petitioners,
V.

MERRICK B. GARLAND, ATTORNEY GENERAL,
Respondent.

On Writs of Certiorari from the United States Court of Appeals for the District of Columbia Circuit

BRIEF OF *AMICUS CURIAE* PROFESSOR MILTON MUELLER IN SUPPORT OF PETITIONERS

Anne M. Voigts
Counsel of Record
Pillsbury Winthrop Shaw Pittman
2550 Hanover Street
Palo Alto, CA 94304-1115
(650) 233-4075
anne.voigts@pillsburylaw.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

STATEMENT OF INTEREST OF *AMICUS CURIAE*[1]

Amicus curiae Professor Milton L. Mueller is an internationally prominent scholar specializing in cybersecurity, data governance, public affairs, internet governance, and national security. Professor Mueller is a Senior Professor at Georgia Institute of Technology, School of Public Policy and the Program Director for Georgia Tech's interdisciplinary master's degree in Cybersecurity. He is also the author of seven books and scores of journal articles. In particular, his books Will the Internet Fragment? (Polity, 2017), Networks and States: The global politics of Internet governance (MIT Press, 2010) and Ruling the Root: Internet Governance and the Taming of Cyberspace (MIT Press, 2002) are acclaimed scholarly accounts of the global governance regime emerging around the Internet.

Dr. Mueller is also the co-founder and director of the Internet Governance Project (IGP), a policy analysis center for global Internet governance. Since its founding in 2004, IGP has played a prominent role in shaping global Internet policies and institutions such as ICANN and the Internet Governance Forum. Founded in 2004, the Internet Governance Project (IGP) has grown to be a leading source of analysis of global Internet policy and Internet resource management that is widely read by governments,

---

[1] Pursuant to S. Ct. Rule 37, no counsel for a party authored this brief in whole or in part and no person or entity other than *amicus* or his counsel made a monetary contribution to its preparation or submission.

industry, and civil society organizations. He has participated in proceedings and policy development activities of ICANN, the International Telecommunications Union (ITU), the National Telecommunications and Information Administration (NTIA), and regulatory proceedings in the European Commission, China, Hong Kong and New Zealand, and has served as an expert witness in prominent legal cases related to telecommunication policy. He was elected to the Advisory Committee of the American Registry for Internet Numbers (ARIN) from 2013 to 2016 and appointed in 2014 to the IANA Stewardship Coordination Group. Dr. Mueller has also been a practical institution-builder in the scholarly world, where he led the creation of the Global Internet Governance Academic Network (GigaNet), an international association of scholars.

This amicus brief explains why, based on Dr. Mueller's decades of experience and research, this Court should not defer to the government's constitutional analysis. As Dr. Mueller explains, the appellate court's analysis gave insufficient weight to American's constitutional right to communicate on their platform of choice and receive information from sources that do not meet with government approval, relied on an inaccurate assessment of the potential threats, and has broad—and negative—ramifications for foreign policy.

SUMMARY OF THE ARGUMENT

The Protecting Americans from Foreign Adversary Controlled Applications Act ("the Act") is

an unconstitutional solution to a perceived problem that does not warrant the extraordinary and unprecedented step of banning an entire digital platform. In its decision upholding the constitutionality of the Act, the Court of Appeals gave "great weight to the Government's evaluation of the facts because the Act implicates sensitive and weighty interests of national security and foreign affairs." *TikTok, Ltd., et al. v. Garland,* __ F.4th __, 2024 WL 4996719 at *13 (D.C. Cir. Dec. 6, 2024). But deference is not the equivalent of an indulgence, excusing all manner of constitutional sins, including what the Court itself called "the absence of 'concrete evidence' on the likelihood of PRC-directed censorship of TikTok in the United States." *Id.* at *20.

Here, that deference prevented the court from fully and properly considering the most essential issues in this case.

First, the appellate court failed to provide a coherent analysis of the scope and scale of the alleged national security risks and whether those risks justify the Act's unprecedented curbs on freedom of expression and Internet access. Instead of conducting a proper balancing test, the court simply agreed that there was a risk and conducted no adequate analysis whether it rose to the level of a national security threat or whether the Act was a proportionate solution. (It does not and it is not.) And while the appellate court purportedly relied on only those facts in the public record, the government's position that the courts (and the public) should trust it to both assess the purported problem and to craft a draconian

solution to it is one that every court, and citizen, should find troubling.

Second, the appellate court's decision focuses so narrowly on TikTok/ByteDance as a company that it fails to meaningfully consider the First Amendment rights of Americans to choose to use TikTok to convey and receive communications. The very nature of these platforms, including the fact that their content is user-generated, and curated according to the platform's expressive choices, means that a law that regulates a specific platform, like this one, is not and cannot be content-neutral. Platforms are not fungible—accountholders on Truth Social participate in a very different discussion than those on BlueSky, for example, just as viewers choose between Fox News and MSNBC—and individuals have the constitutional right to choose which platforms to participate in and which voices to listen to. That right exists under the First Amendment regardless of who owns a particular app and whether it can be purportedly influenced by a foreign government. At stake here is the ability of Americans to access an information source, and any legal rationale for governmental interference with that right opens the door to a broad range of First Amendment incursions.

Third, upholding this law would set a damaging precedent for freedom of expression in digital media. The United States has potentially far more to lose than it has to gain it by using a blunt force instrument—like the blanket ban here—to mitigate

whatever national security risks that online platforms may pose. Affirming this departure from core American values and constitutional protections will likely harm the United States' global standing and jeopardize some of its foreign policy goals—the very opposite of Congress's intended effect. This Court should reverse.

ARGUMENT

I. This Court Should Not Defer to the Government's Constitutional Analysis

The Court of Appeals upheld the Act because "[t]he government's evaluation of the facts, is entitled to deference." *TikTok*, 2024 WL 4996719 at *13. This reliance on the federal agencies' campaign against TikTok, however, fatally undermines that decision. While our military and intelligence agencies are sincerely attuned to the detection of national security threats, they do not have any special insight into how we should balance the individual rights of free expression on the one hand and the collective security risks allegedly posed by a social media app on the other. On the contrary, these agencies are focused on security objectives to the exclusion of all other objectives. Their goal is to maximize the relative power of the United States and to minimize any threats posed by our adversarial relationship with China, and they have little incentive to calibrate the risk, let alone to do so to constitutional standards.

That is not surprising. Protecting free speech and open competition in the social media market is not part of their mandate. As a result, the FBI, the NSA,

and the military have in the not-too-distant past used national security claims to engage in unconstitutional surveillance, disruption of political movements, and illegitimate censorship. In all these cases, their actions were based on their own internal determination of what constituted a threat to national security, assessments that were probably made with the utmost sincerity. But courts have repeatedly reversed those assessments precisely because those agencies' built-in bias could not be squared with constitutional mandates.[2]

---

[2] For example, the Department of Defense insisted that the publication of the Pentagon Papers by the New York Times was a threat to national security. *New York Times Co. v. United States,* 403 U.S. 713, 714 (1971). The Supreme Court overruled them. *Id.*

In other cases, the courts have conducted balancing tests that weigh the severity of the threat against the constitutional rights at stake. And outside of the First Amendment context, in several cases related to the war against terrorism and the Guantanamo Bay detainees, the military's handling of terrorist suspects who clearly raised serious national security concerns, was moderated by the courts. *E.g., Boumediene v. Bush*, 553 U.S. 723, 792 (2008) (concluding that procedures for reviewing detention of individuals designated as enemy combatants "effect[ed] an unconstitutional suspension of the writ" of habeas corpus)*; Hamdi v. Rumsfeld*, 542 U.S. 507, 532–33 (2004) (plurality op.) ("'the risk of an erroneous deprivation' of a detainee's liberty interest is unacceptably high under the Government's proposed rule"); *see also, e.g., United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 316–17 (1972) (holding that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch"). It is not at all uncommon, in other words, for the

The appellate court here, however, seemed oblivious to the checkered record of Congress in the development of this Act. Its hearings on TikTok were a political circus that repeatedly sought to characterize TikTok's Singaporean CEO as a Chinese citizen or CCP member – all to reap political capital from anti-China sentiment. To overcome objections from Congressional supporters of free speech, House Republicans had to push the Act into a $95 billion foreign aid package that had to be "passed as quickly as possible." In so doing, Congress offered no reasons for singling out TikTok from every other social media platform that collects user data and contends with foreign influence operations. This is not a weighty deliberative process that deserves deference.

It is the Supreme Court's job to provide the balance between national security claims, populist political trends, and valued civil liberties, especially if the security claims may be or in fact are inflated for political or strategic purposes. The Court of Appeals shirked that duty. It deferred to the threat assessment of the Executive Branch and Congress without conducting any critical substantive analysis of the risk and without properly performing any balancing test. That deference is even more questionable given the factual, legal, and logical weaknesses in the Justice Department's argument that TikTok is a major security threat. *See infra.*

---

courts to rule that the threat assessments of the FBI, the military, or the intelligence agencies do not justify compromising constitutional rights.

II. Americans Have a Constitutional Right To Communicate on Their Platform of Choice and To Receive Information From Foreign Sources

The appellate court's decision failed to adequately consider the most critical First Amendment issue at stake in this case: the right of Americans to choose TikTok as a means of speaking and being spoken to (with other Americans as well as foreigners). The appellate court's contrary decision is deeply inimical to the principles of freedom of expression and liberal democracy.

As this Court has repeatedly recognized, those principles were founded in a rejection of the prior historical practice of requiring governmental permission for a press to operate. As early legal historians recognized, "'[t]o subject the press to the restrictive power of a licenser, as was formerly done, both before and since the revolution, (of 1688) is to subject all freedom of sentiment to the prejudices of one man, and make him the arbitrary and infallible judge of all controverted points in learning, religion, and government.'" *Near v. State of Minnesota ex rel. Olson*, 283 U.S. 697, 733–34 (1931) (quoting Blackstone); *see also id.* (quoting Madison on the value of a free press).

Americans can use the Web, email, other social media apps like Twitter, BlueSky or Facebook, streaming video, podcasts, or books to access any source of information in the world. The exercise of this right is not and should not be contingent on a determination by their government that the content

they access is not "manipulated by a foreign adversary." Some content on any platform could in fact be manipulated to some degree. The remedy, however, is not a preemptive ban. *Id.* at 720 (noting that only subsequent punishment that falls within constitutional limits is "the appropriate remedy"). Instead, it is for Americans, not their government, to decide what they see or hear or read.

Implicit in this freedom is faith in the resilience of democracy and the rationality and sovereignty of the American people. They can make up their own minds about what to believe, and they should be allowed to decide for themselves what ideas or sources are useful or threaten their security. If an American citizen has a right to access a website run or influenced by the Chinese Communist Party, or to read a book or access a podcast whose producers may be sympathetic to or even covertly paid by the Chinese government, why does that citizens not also have a right to access the TikTok app? *See Red Lion Broadcasting Co. v. Federal Communications Commission*, 395 U.S. 367 (1969) (recognizing that the First Amendment protects the public's right to receive information, not just the broadcaster's right to speak). That is particularly true given that, as both the government and the court have conceded, it is not run by the CCP, and the alleged national security risk is purely prospective in nature, based on concerns that at some point the app might be indirectly influenced by the Chinese government in the future.

In *Lamont v. Postmaster General,* 381 U.S. 301, 307 (1965), this Court invalidated a federal law

requiring recipients of "communist political propaganda" to request its delivery. It did so on the grounds that the statute sought to impermissibly "control the flow of ideas to the public" through "a regime … at war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment." *Lamont*, 381 U.S. at 306-07. Moreover, it did so even though the law in question did not impose an absolute bar on receipt of such material. *Id.* Instead, it concluded, the requirement that an addressee must request that his or her mail be delivered in order to receive that mail would likely mean that "*any* addressee is likely to feel some inhibition" about making such a request. *Id.* (emphasis added). And that state interference with the individual's right to access ideas could not be squared with the Constitution.

The court of appeals here tried to dismiss *Lamont* based on a tangled and counterfactual argument that contradicts the very rationale for the Act. The court contended that the Act was *not* an effort to "control the flow of ideas to the public," *TikTok,* 2024 WL 4996719 at *18, even though it repeatedly justified the Act based on the need to prevent Americans from being exposed to an adversary government's ideas. Specifically, the court wrote: "Across the globe, the PRC seeks to 'promote PRC narratives ... and counter other countries' policies that threaten the PRC's interests." *Id.* at *37.

Additionally, the appellate court asserted that the law overturned in *Lamont* "drew a viewpoint-based distinction based on whether the government

deemed mailed material 'communist political propaganda," but that the Act here does not. *Id.* at *35. The court contended that the Act "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," but instead sought "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." *Id.*

That argument contradicts itself. The whole point of influencing a communications medium is to alter "the mix of views" on it, here, by allegedly promoting views favorable to China's government and/or suppressing critical ones. Thus, from the get-go, the entire national security rationale for the ban or forced divestiture is based on a "viewpoint-based distinction." It is an attempt to control (or prevent) the flow of what the federal government claims might be Chinese-approved ideas to the American public. (For the reasons set forth below, whether any purported content manipulation is "covert" or not is really a red herring.)

Based on the premise that mere exposure to these ideas endangers the very fabric of American institutions (like the arguments in *Lamont* about Soviet communist viewpoints), the Act overrides the choices of tens of millions of Americans regarding which social media app they are allowed to use. What logic would justify protecting Lamont's choice to receive communist literature advocating the

overthrow of America's capitalist state in 1962, but not 150 million American users' right to access entertaining videos on TikTok in 2024? The principle behind this restriction of their First Amendment rights could be used to justify a Chinese-style national Internet filtering regime regulating Americans' access to many other foreign websites and online services.

Nevertheless, the appellate court defended the Act's intrusion on core First Amendment principles by claiming that doing so is essential to vindicating those principles. Put differently, the court argued that it had to gut the First Amendment in order to preserve it. Specifically, the appellate court defended banning TikTok by contending that "[a]t 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." 2024 WL 4996719 at *17. There are two problems with this rationale. First, it invokes an individual's right to decide which "ideas and beliefs [are] deserving of...consideration" in support of a law that would strip American citizens of that right. Second, it suggests that any editorial selection, promotion, or suppression of content on a platform is at odds with the First Amendment, as opposed to being protected by it.

This Court of course held the contrary in *NetChoice v. Moody*, 603 U.S. 707 (2024). *All* social media platforms engage in the promotion, selective display, and suppression of content, and the Supreme Court has repeatedly recognized that such editorial control is a protected form of expression. *Moody,* 603

U.S. at 734 ("The government may not, in supposed pursuit of better expressive balance, alter a private speaker's own editorial choices about the mix of speech it wants to convey"); *Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241, 258 (1974) ("The choice of material to go into a newspaper…constitute[s] the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time").

Moreover, most users exercise their First Amendment rights not by publishing things themselves but by making choices among various providers of editorial control; i.e., they patronize different newspapers, different social media platforms, or different streaming channels. The Act infringes on that right by telling Americans that they do not have the right to select a specific information source. And it restricts this right not because another government is engaged in content manipulation, but because our government thinks it could potentially do so at some indefinite time in the future. In essence, the government is telling the Court (and its citizens) to trust it to know what is best, and to privilege its concerns about potential future harm over the Act's actual, direct impact on speech and the constitutional limits on such government action that have existed for more than two centuries.

III. The Court of Appeals Relied on An Inaccurate Assessment of the Purported Threat Scenario

As noted above, the court offered two justifications for this sweeping and unprecedented law: first, it asserted that the Act was constitutional because "a foreign government threatens to distort free speech" in the United States by "covert manipulation" of user exposure to the content placed on one app, TikTok.[3] 2024 WL 4996719 at *19. Second, it contended that concerns about the collection and potential exfiltration of user data provide an alternative justification. *See infra.* Neither warrants such a substantial retrenchment of core constitutional rights.

With respect to the first justification, the court's reasoning goes, it must infringe on free speech to preserve it. There are two fundamental problems with that: first, the evidence of content manipulation is thin at best. As the decision notes, "the Government

---

[3] Instead, the Court relies on the Government's claim "that ByteDance and TikTok Global have taken action in response to PRC demands to censor content outside of China" and that "ByteDance and its TikTok entities 'have a demonstrated history of manipulating the content on their platforms, including at the direction of the PRC.'" *Id.* But there is no attempt to calibrate or quantify the scale of the problem. Have there been one or two incidents of deferring to PRC demands, or hundreds? Did it occur, if at all, in the early days of ByteDance's globalization, and has it since ended, or did it happen recently (almost certainly, the former)? What kind of content was involved? Moreover, virtually all platforms have a demonstrated history of manipulating content on their platforms, sometimes at the request of governments.

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." 2024 WL 4996719 at *19. Second, in America's diverse media environment, the potential for content manipulation does not rise to the level of a national security threat. The government's (and the court's) threat assessment depends upon the idea that distortions of free speech on one of many platforms in the United States, if or even when it might happen, is capable of bringing down the government or, at a minimum, seriously impeding its military and foreign policy actions—and that the only possible solution for that threat is divestiture. But a sufficient link between potential "content manipulation" on one (and only one) platform in the United States and consequences threatening national security is never really demonstrated by either the government or the court. It is simply assumed. The Constitution demands more.

A. The Dog That Didn't Bark: The Government's Allegations of "Covert Manipulation" Do Not Hold Up

Central to the appellate court's justification of a ban is the idea that Chinese influence on TikTok's recommendation algorithm would be "covert," that is, invisible and undetectable to users. The court presented "covert content manipulation" by China as an act of interference with the free speech of TikTok users and, in an Orwellian twist, justified one government's ban on access to the app as a permissible way of protecting TikTok users from another

government's potential interference. The fact that TikTok's American user base has grown at a record pace and that those users apparently do not feel oppressed or limited did not seem to matter to the court.

That is not the only flaw with this line of reasoning. First, neither Congress nor the security agencies have any evidence that the "covert manipulation of content" they fear is actually happening on the version of TikTok used by Americans. This fact by itself raises serious challenges to sufficiency of the state's threat scenario. If covert manipulation of content on TikTok were truly a powerful weapon in the hands of the Chinese, and if TikTok/ByteDance were indeed highly susceptible to implementing such manipulation, the PRC government's failure to use it after seven years of the apps' presence in the U.S. is difficult to explain.

Since 2018, the United States has unleashed a series of hostile policy actions targeting China, including, inter alia, steep tariffs, bans on the export of advanced semiconductors, the expulsion of Chinese telecommunications firms from the U.S. market, and the approval of $2 billion in arms sales to Taiwan. If TikTok were indeed a powerful weapon capable of undermining United States' actions inimical to China's interests, surely the period 2018 – 2024 would have been the time to use it. Added to this interesting case of the dog that did not bark, there are thousands of videos on TikTok that are critical of China or that raise issues that the PRC does not want aired, like the status of Uighurs or the independence of Taiwan.

The government's threat assessment in support of this sweeping and unprecedented law is based entirely on fears of something that "could happen" but inexplicably *isn't* happening precisely when one would expect it to. As a result, in its attempt to find a major security threat, the Justice Department is forced to posit a contradictory scenario: the content manipulation could be so "covert" that no one can tell it is happening, yet so powerfully influential that it threatens national security. (That scenario also rests on a host of unsupported assumptions about what societal effects would occur if such a change did happen. *See infra.*)

Consider a parallel. It is well known that the movie "Top Gun: Maverick" eliminated Japanese and Taiwanese patches on Maverick's bomber jacket due to indirect pressure from the Chinese government. Chinese censors control which movies are allowed into its large and lucrative market, and positive references to Japan and Taiwan would exclude them from the Chinese market. There is evidence that several other Hollywood blockbusters have followed the same pattern. Alex Hollings, 4 times movies changed because of Chinese pressure, The Mighty. October 30, 2020. https://www.wearethemighty.com/mighty-movies/hollywood-china-censorship/.

When Hollywood movie producers avoid narratives or characters that would offend the Chinese government, lest their big budget movies be excluded from the Chinese market, this is an unfortunate constraint on their speech, but it is not undetectable, and it does not rise to the level of a

national security threat. Under the court's logic, however, the United States government would be justified in banning these movies in the United States to save us from China's "covert content manipulation." In other words, the government would protect freedom of speech by eliminating it. And in the case of TikTok, it would do so based on the potential for future content manipulation, rather than proof of actual, current manipulation unique to TikTok and rising to the level of a national security threat.

B. The Court's Concerns With Covert Content Manipulation Depend On A Fundamental Misunderstanding Of How Social Media Platforms Function

These fears of "covert content manipulation" betray a fundamental lack of knowledge about social media, content recommendation algorithms, and the digital media market generally. They suggest that indirect PRC interference in TikTok's content selections could be impossible to detect, let alone counter, but still, at the same time, have extraordinary powers to manipulate the minds of millions of Americans. These conclusions are not grounded in any social psychological research about social media effects, which shows that algorithms detect and respond to preferences, and can amplify or diminish pre-existing attitudes, but do not create them.

The appellate court's decision erroneously thinks of social media platforms as a broadcast station or newspaper that conveys one uniform, regulated

stream of messages to the user. In fact, there are tens of millions of content originators on TikTok global, and most of them are Americans. TikTok's recommendation algorithms do not create content, they make decisions about which of the millions of short videos produced by these users another user is likely to want to see. The TikTok algorithm is successful precisely because it incorporates the actual interests of its users as part of its expressive choices. The stream of videos suggested on the "For you" channel will thus be different for every user; there is no broadcast of a party line. Even assuming that the PRC government were to place pressure on ByteDance to suppress or promote specific videos, there is no guarantee of impact. TikTok users respond to what they are presented by quickly swiping away from videos that do not immediately catch their attention, and most TikTok users are not that interested in political content.

The influence the government and the court fear could come about in two ways. One would be a systematic transformation of TikTok into a fully utilized PRC influence operation. The other would be a limited set of acts suppressing or promoting a few selected items of content, in response to pressure from Beijing.

The first possibility, a sudden and complete transformation of TikTok into a state-directed influence operation, is not a serious risk. First, it would be easily detectable; second and more importantly, it would undermine the very basis of

TikTok's ability to make money by attracting, engaging, and retaining users.

If TikTok's recommendation algorithm is systematically manipulated to provide material that the PRC wants users to see, rather than its own expressive choices and users' own interests and preferences, engagement will decline and so will the number of users. Chinese government-produced material in English is readily available on websites, in books, and on television stations. Influencers who have been secretly paid by the Chinese exist on YouTube, X, and elsewhere. Of course, those outlets do not have 170 million Americans following them. TikTok is popular in the American market because its algorithm incorporates its users' own interests. An algorithm tuned to CCP propaganda will not. If such an algorithm were implemented, TikTok's growth and advertising revenue would decline, users will move to other platforms, and any alleged messages will fall on deaf ears. Thus, any potential systematic manipulation of TikTok's algorithm for CCP political purposes would be constrained by commercial imperatives and user choice. And any isolated manipulation would also not rise to the level of a national security threat.

The recent history of Twitter's transformation into "X" provides a real-world example of a social media platform's transformation. Elon Musk's acquisition of Twitter enabled him to promote his own messages and to alter the recommendation algorithms to be less restrictive of content the previous owners suppressed. Users and advertisers noticed. Many

conservatives welcomed Musk's changes, many liberals and progressives hated them. X has suffered an advertiser boycott, a decline of 8% in U.S. users, and a decline of 15% worldwide.[4] Its stock market value dropped from $5.7 billion in 2022 to $673 million in December 2024.[5]

The Twitter/X case proves that a major change in the type and ideology of content promoted by a social media app will be noticed and will trigger negative reactions, less engagement, and abandonment if the changes do not reflect what existing users want to see. The idea that TikTok could undergo a similar transformation at the hands of the Chinese state without anyone noticing is absurd.

The second possibility, a few acts of suppression or promotion, is more plausible. But by the same token, those limited interventions could only have very limited effects on public opinion in America. once one situates TikTok in the larger American media ecosystem. TikTok does not have anything close to a monopoly on Americans' attention. Users and researchers will detect the suppression of content critical of China and this will trigger comment and criticism. Manipulating a few items of discourse on

---

[4] Kat TenBarge, X Sees Largest User Exodus Since Musk Takeover, https://www.nbcnewyork.com/news/national-international/x-largest-user-exodus-since-elon-musk-takeover/5982438

[5] Jose Enrico, X Likely to Lose More Users in 2025, https://www.techtimes.com/articles/308735/20241216/x-likely-lose-more-users-2025-post-election-exodus-projected-have-continuous-ripple-effect.htm

TikTok is not the same as manipulating all discourse on TikTok, much less all public discourse in the rich and diverse media environment of the United States. Thus, while the possibility of some form of influence on any social media platform cannot be categorically ruled out, the government has drastically inflated the potential risk, contending that the possibility of introducing minor biases in the selection of content in the For You feed poses a threat to the entire country.

Inexplicably, the court dismissed the idea that the United States government (and any other domestic source of comment and opinion) can respond to PRC-inspired content biases with exposure and critical commentary. Instead, it brushes that idea off as naive with no real evidence or reasoning. This is disturbing because the Constitution affirms that the answer to problematic speech is more speech, not less. *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring) (when the government objects to speech, "the remedy to be applied is more speech, not enforced silence"). The concept that false or manipulative speech can be countered and criticized is a fundamental premise underlying the First Amendment. A society that privileges and protects free speech is more resilient than one that does not precisely because the affected citizens have access to diverse, contending ideas. Indeed, videos posted on TikTok (and on any other media) can be and often are challenged, criticized, commented upon, and incorporated into other videos.

In dismissing any appeal to counter-speech as naive, the court provided an alarming rationale for

restricting core free speech rights. If the answer to false or propagandistic content is not more speech, the logical next step is that the government should decide what speech is safe to share—and that courts should, as in China, allow the government to decide. But that is just a change in terms of who exerts control, not a challenge to the propriety of that control, and cannot be squared with the First Amendment.

In short, the court's contention that interfering with Americans' choices of social media platforms "protects free expression" combines hostility to free expression with a factually flawed analysis. The court assumed that TikTok's users are a captive audience with no agency, and that only government action can protect their choice. It presumed that the potentially biased selection of a few items of content on one of many information sources will rise to the level of a national security concern warranting infringement on fundamental constitutional rights. These assumptions, critical to its whole argument, demonstrate that the court simply did not understand the dynamics of free speech in a free and open social media market. Free expression hinges on the ability of users to vote with their feet in the adoption of apps, publications, and groups. Americans have that choice with respect to TikTok, regardless of who owns it or how much external pressure it is subjected to. Interfering with that right interferes with their exercise of free expression.

C. The Appellate Court's Reliance on Foreign Ownership Limits in Radio Was Also Wrong

The appellate court decision asserted that the Act's "emphasis on ownership and control follows a longstanding approach to counter foreign government control of communication media in the United States." 2024 WL 4996719 at *20. That conclusion depends on a fundamental misunderstanding of United States regulatory practice and legal precedents. To begin with, all the law and regulatory precedents apply exclusively to radio frequency ownership, not to "communications media" generally. (Of course, radio licenses are not involved in this case.) Outside of that context, United States law and regulation has favored unlimited access to foreign content and openness to foreign investment, particularly since the advent of the Internet.

Legal ownership restrictions on radio frequencies date back to the 1912 Radio Act, when radio was primarily a means of telegraphic communication, particularly important for navies. The government's security interest was rooted in its concern about ship-shore and ship-ship communications along United States coasts and the possible use of radio telegraphy by spies and foreign navies.[6] Accordingly, the U.S. Navy from 1906 - 1909

---

[6] Sidak dates the origins of these concerns to the use of wireless communications by the Japanese Navy in the 1904 Russo-Japanese War. J. Gregory Sidak, Foreign Investment in Telecommunications. Working Paper Prepared for the

advocated for a military monopoly on all radio frequencies in the U.S., an overreach that was, fortunately, resisted by civil society and Congress.

At the behest of the Navy, however, the 1912 Act did restrict the award of radio licenses to foreigners. Donna M. DiPaolo, Executive Research Project, Foreign Ownership Restrictions in Communications and "Cultural" Trade: National Security Implications. Thesis, The Industrial College of the Armed Forces, https://apps.dtic.mil/sti/tr/pdf/ADA314840.pdf. The target was not "foreign propaganda," however, but the prevention of "alien activities against the U.S. Government during wartime"; *i.e.*, the use of radio to plan and coordinate attacks. *Id.* In line with this rationale, the Act allowed the government to seize radio stations during wartime (which it did during World War I). Unlike a software app distributed over the Internet, the possession of radio licenses would have given foreign powers control of a communications infrastructure in the United States. The more liberal licensing conditions of the 1912 Act, which excluded foreign ownership but allowed easy access to licenses for civilians, paved the way for American leadership in broadcasting and other civilian applications of radio technology.

The subsequent 1927 Radio Act was motivated primarily by an attempt to regulate the competition for radio frequencies generated by the rise of commercial broadcasting. It retained the licensing

---

American Enterprise Institute for Public Policy Research, presented November 1995.

restrictions of the 1912 Act, which in turn were tightened a bit by the Communications Act of 1934.[7] The motive, however, was less about foreign content and more about the limited number of broadcast frequencies and the fear that foreign owners might dominate the industry. Control of a radio frequency by a foreign company necessarily excludes an American company from holding the same frequency, whereas the offering of a software app that provides content via the Internet does not exclude any other company, foreign or domestic, from offering a competing app. There is no exclusive occupation of a scarce resource.

In 1958, a court challenge pushed the FCC to narrow its view of the national security interest in radio in a way that mirrored the original focus on alien activities against the U.S. government during wartime. *Noe v. FCC*, 260 F.2d 739 (D.C. Cir. 1958). Relying on the legislative history of the Radio Act of 1927, the court rejected contentions that section 310 was designed to block "foreign influence" in U.S. broadcast content. In 1974, Congress revised section 310, limiting the section's applicability to common carrier, broadcast and aeronautical radio services, areas which at that time were seen as most directly affecting national security.

Thus, far from having a "long-standing" policy of content-based exclusions of foreign owners in communications, the limits on broadcast ownership have been narrowly limited to concerns about alien

---

[7] Holding companies had been used to get around the restrictions, and this "loophole" was closed.

control of radio frequencies in times of conflict or war. Cable television, direct broadcast satellite, subscription television, streaming video, websites, and software applications are not and never have been subject to foreign ownership restrictions in the United States. Even in broadcasting, the FCC over a decade ago decided to permit, on a case-by-case basis, greater foreign ownership of US broadcast stations, resulting in instances where 100% foreign ownership of U.S. broadcast stations have been permitted. Many large U.S. broadcast companies now have foreign ownership in excess of the 25% allowed by Section 310(b)(4) of the Communications Act. Most importantly, there have been *no* ownership restrictions or access restrictions on websites or other content that can be accessed over the Internet. Contrary to the court's conclusion that the Act was consistent with prior regulations, the TikTok ban is a radical departure from prior U.S. policies regarding Internet freedom, access to foreign content, and the free flow of data.

D. The Threat Of Data And Espionage Also Does Not Warrant Disregarding The Constitution's Bar On Government Regulation Of Speech

As amicus has explained elsewhere, an extensive analysis of the alleged risks posed by the potential for Chinese government access to the data generated by TikTok users does not substantiate those concerns. *See, e.g.,* Mueller and Farhat, "TikTok and U.S. National Security," Georgia Tech Internet Governance Project, Jan. 2023, Section 3 (p. 18-22). https://www.internetgovernance.org/research/tiktok-

and-us-national-security/. (Indeed, both American Presidential candidates in 2024 had TikTok accounts, apparently not concerned about yielding privileged or damaging information to the Chinese.)

Specifically, as amicus has explained, TikTok's data collection practices are consistent with those of other social media platforms, and whether a foreign power's access to this data could pose a national security risk depends entirely on who the user is. *Id.* There is a plausible risk, in other words, only if the TikTok user is an individual whose actions or locations can have an impact on US national security, and that user participates in TikTok in a way that allows the person to be identified and tracked, or exposes valuable, confidential information about the U.S. government or its military and intelligence agencies. *Id.* To monitor persons of interest on TikTok (and other social media), the Chinese government need not have any special legal or political authority over TikTok. *Id.* To the contrary, as amicus has explained, whatever intelligence value a record of TikTok usage has can for the most part be harvested without any cooperation from the company, and that the same risks apply to all social media. *Id.*

The appellate court seemed not to understand the simple fact that most of the user activity on TikTok – and on all social media – is public and can be gathered and analyzed simply by subscribing to and monitoring the service or employing tools to "scrape" the public data. *Id.* Indeed, this is how the Chinese already monitor dissidents and persons of interest in other countries. *Id.* This is also why laws and

organizational policies already exist to prevent people in sensitive positions from having public profiles on social media. Sensibly, these restrictions apply to all social media, not just TikTok, because all of them can reveal information about user activity, locations, likes, comments and connections. There is nothing special about TikTok in this regard. Any usage of social media in the wrong way by people in sensitive positions poses risks. There is also a risk that this data can be exposed through a breach or sold. Worldwide, twenty-nine million Facebook accounts were breached in 2018. A security incident compromised 110.8 million Google accounts and exposed password reset links, 2FA codes, and employee credentials. Most of those risks affect individual privacy, not national security, however. Intelligence operatives and military leaders are not stupid enough to post videos of advanced weapons systems, secret plans, troop movements or passwords on TikTok or YouTube.

Mitigations short of a ban, such as policies to prevent military personnel, intelligence agency employees, and government employees from using social media or using it in the wrong way, are more appropriate, more effective, and less constitutionally problematic. The U.S. law limiting the sale of location data by data brokers, which allowed adversarial governments and practically anyone else to buy the kind of data, is another constructive step. Finally, general data privacy laws that prevent companies from giving private user data to anyone and penalize them for doing so are a far more constitutionally calibrated alternative.

IV. The Manner In Which the United States Regulates Speech Domestically Has Broad Ramifications For Foreign Policy

Finally, the manner in which Congress chooses to regulate foreign-owned online platforms has broad ramifications for foreign policy.

To begin, the United States has consistently advocated for free speech both domestically and abroad. Even (or especially) when the government invokes national security concerns as a basis for limiting speech, the Supreme Court has long upheld the full scope of First Amendment protections. That is, in such circumstances, the government still "carries a heavy burden of showing justification for the imposition of such a restraint." *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971). As Justice Holmes once observed: "[A]s against dangers peculiar to war, as against others, the principle of the right to free speech is always the same. It is only the present danger of immediate evil or an intent to bring it about that warrants Congress in setting a limit to the expression of opinion where private rights are not concerned." *Abrams v. United States*, 250 U.S. 616, 628 (1919) (Holmes, J., dissenting).

Moreover, the costs of such regulations are not limited to the immediate constitutional ones. The perception of the United States as a beacon of freedom will be diminished—and its foreign policy less successful—if the government simply bans an expressive platform without courts requiring a sufficiently exacting showing by the government that

such a ban is necessary and that other, less restrictive solutions are not adequate. Imposing a flat ban on speech is more in line with an authoritarian model of government whose standards and values are markedly different from the United States. Take, for example, China's extraordinary levels of censorship, which stand in stark contrast to the United States' commitment to the First Amendment.[8] And history has not been kind to those rare instances in which the United States has used broad national security concerns to justify a departure from its founding principles of liberty and freedom for all. *See Korematsu v. United States*, 65 S. Ct. 193 (1944).

In imposing a flat ban, the United States has more to lose than moral high ground. Such bans may also invite significant retaliation from important trade partners that jeopardize national security in even more profound ways than the online platform itself. Moreover, permitting Congress to institute a blanket ban on online platforms from other countries risks setting a dangerous precedent globally. Will other countries follow suit and eschew diplomacy in favor of siloing their citizens from foreign products? And, of course, endorsing such a policy abroad risks a trickle-down effect on domestic policy.

In sum, the United States has potentially far more to lose than it has to gain if it unnecessarily uses a blunt force instrument—like a ban—to mitigate the unique national security risks that online platforms

---

[8] Freedom on the Net 2021, FREEDOM HOUSE (visited Dec. 27, 2024), https://freedomhouse.org/country/china/freedom-net/2021.

may pose. This Court should not depart from core American values and constitutional protections. Doing so will likely harm the United States' global standing and jeopardize foreign policy—the very opposite of Congress's intended effect.

CONCLUSION

For these reasons, the Court should find the Act unconstitutional.

Respectfully submitted,

Anne M. Voigts
Counsel of Record
Pillsbury Winthrop Shaw Pittman
2550 Hanover Street
Palo Alto, CA 94304-1115
(650) 233-4075
anne.voigts@pillsburylaw.com

Counsel for Amicus Curiae