ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024
Case No. 24-1113 (and consolidated cases)

# United States Court of Appeals for the District of Columbia Circuit

**TIKTOK INC. AND BYTEDANCE, LTD.,**

*Petitioners,*

**v.**

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

*Respondent.*

*caption continued on inside cover*

ON PETITIONS FOR REVIEW OF CONSTITUTIONALITY OF THE PROTECTING AMERICANS FROM FOREIGN ADVERSARY CONTROLLED APPLICATIONS ACT

## BRIEF FOR STATES OF MONTANA, VIRGINIA, AND 19 OTHER STATES AS AMICI CURIAE IN SUPPORT OF RESPONDENT

AUSTIN KNUDSEN
*Attorney General of Montana*
CHRISTIAN B. CORRIGAN
*Solicitor General*
PETER M. TORSTENSEN, JR.
*Deputy Solicitor General*
MONTANA DEPARTMENT OF JUSTICE
215 North Sanders
P.O. Box 201401
Helena, MT 59620-1401
(406) 444-2026
peter.torstensen@mt.gov

JASON S. MIYARES
*Attorney General of Virginia*
ERIKA L. MALEY
*Solicitor General*
KEVIN M. GALLAGHER
*Principal Deputy Solicitor General*
MICHAEL DINGMAN
*Assistant Solicitor General*
OFFICE OF THE ATTORNEY GENERAL
202 North Ninth Street
Richmond, VA 23219
(406) 786-2071
KGallagher@oag.state.va.gov

*Counsel for the States of Montana and Virginia*
*(Additional Counsel listed after signature block)*

**BRIAN FIREBAUGH, ET AL.,**

*Petitioners,*

**V.**

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

*Respondent.*

---

**BASED POLITICS INC.,**

*Petitioner,*

**V.**

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

*Respondent.*

## CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), the undersigned counsel of record certifies as follows:

A. **Parties and Amici**: All parties, intervenors, and amici appearing before this Court in the three consolidated cases are listed in the Public Redacted Brief for Respondent.

B. **Rulings Under Review**: These petitions seek review of the *Protecting Americans from Foreign Adversary Controlled Applications Act*, Pub. L. No. 118-50, div. H (2024). There are no prior rulings under review.

C. **Related Cases:** There are no related cases to amici's knowledge.

*/s/ Peter M. Torstensen, Jr.*
PETER M. TORSTENSEN, JR.

## TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## CASES

**CONSTITUTIONAL PROVISIONS**



**STATUTES AND RULES**



**OTHER AUTHORITIES**

## INTEREST OF AMICI CURIAE

Amici curiae are the State of Montana, Commonwealth of Virginia and 19 Other States ("Amici States"). Amici States have a compelling interest in ensuring that the law protects their citizens from deceptive and harmful business practices. Petitioner TikTok, Inc. ("TikTok") intentionally engages in deceptive business practices which induce individuals to share sensitive personal information that the Chinese Communist Party can easily access. Amici States file this brief in support of Respondent under Federal Rule of Appellate Procedure 29(a)(2).

## SUMMARY OF ARGUMENT

TikTok is a social media platform that hosts and promotes short videos created and uploaded by users. Last year, TikTok was the second most downloaded mobile application worldwide, generating 654 million downloads over the course of the year. As of early 2024, the United States had the world's largest TikTok audience, with approximately 150 million users on the platform.

TikTok aggressively acquires the personal data of its users. Like other social media sites, TikTok learns users' preferences and uses that information to serve targeted content. To do so, TikTok collects sensitive information on each user; as each user scrolls through TikTok, the app

gathers information on that user's interests, locations, type of phone used, apps downloaded, contacts, content created, facial features, voice prints, and even "where [their] eyes are looking on [their] phone[s]."[1] And, like other social media sites, TikTok is addictive. Public health studies have revealed the addictive nature of TikTok and outlined consequences of that addiction, "particularly in transitional-age youths and adolescents."[2]

TikTok, however, is unlike other social media companies in that its parent company—ByteDance Ltd.—is a Chinese company subject to Chinese law that has admitted to using data gathered through TikTok to surveil Americans. The Chinese Communist Party, the political party with unchallenged control of the People's Republic of China, exercises overwhelming influence over ByteDance. TikTok is a valuable tool for conducting corporate and international espionage, and it may allow the

---

[1] A. Thomas, *Cotton issues TikTok warning, cites national security concerns*, N.W. ARK. DEMOCRAT GAZETTE (Nov. 22, 2022), https://tinyurl.com/2kdhxejc; *see also* S. Perez, *TikTok just gave itself permission to collect biometric data on US users, including "faceprints and voiceprints,"* TECHCRUNCH (June 3, 2021) https://tinyurl.com/5n7y2mrw.

[2] Sch. of Pub. Health, *What Makes TikTok so Addictive?: An Analysis of the Mechanisms Underlying the World's Latest Social Media Craze*, BROWN UNDERGRADUATE J. OF PUB. HEALTH (Dec. 13, 2021), https://tinyurl.com/4fp3ymkb.

Chinese Communist Party to track the real-time locations of public officials, journalists, and other individuals adverse to the Chinese Communist Party's interests. Allowing TikTok to operate in the United States without severing its ties to the Chinese Communist Party exposes Americans to the risk of the Chinese Communist Party accessing and exploiting their data.

Press, state and federal agencies, watchdogs, and governments around the world have recently sounded the alarm about TikTok's connection to the Chinese Communist Party. States launched consumer protection investigations into TikTok's activities. Montana even took the bold step of banning TikTok unless it severed its dangerous ties to the Chinese Communist Party. TikTok sued Montana, claiming that only Congress has the power to address data security concerns with a company controlled by a hostile foreign power. *See TikTok, Inc. v. Knudsen*, No. 9:23-cv-61 (D. Mont. May 22, 2023).

So Congress acted. In April, it passed the *Protecting Americans from Foreign Adversary Controlled Applications Act* ("the Act"), Pub. L. No. 118-50, div. H (2024), requiring ByteDance to divest TikTok from its

Chinese Communist Party ties. *See* Sec. 2(c)(1). But TikTok challenged *this* government action as well.

TikTok's Petition for Review confirms that its core technology and infrastructure are ultimately controlled by the Chinese Communist Party. Pet. for Rev., Const. of Protecting Ams. from Foreign Adversary Controlled Applications Act ("TikTok PFR") at 19 ¶ 29, *TikTok Inc., et al. v. Garland*, No. 24-1113 (D.C. Cir. May 7, 2024). TikTok thus claims that the First Amendment protects the right of the Chinese Communist Party to spy on Americans. But the Act doesn't trigger First Amendment scrutiny because it neither targets "conduct with a significant expressive element" nor "has the inevitable effect of singling out those engaged in expressive activity." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706-07 (1986).

Even if the Act triggers First Amendment scrutiny, this Court should apply *United States v. O'Brien*, 391 U.S. 367 (1968), which addresses regulated nonspeech conduct with a speech element. Alternatively, this Court should treat the Act like a content- and viewpoint-neutral "time, place, or manner" restriction. Either way, this Court applies a nearly identical form of intermediate scrutiny analysis. *See Ward v.*

*Rock Against Racism*, 491 U.S. 781, 798 (1989) ("[W]e have held that the *O'Brien* test in the last analysis is little, if any, different than the standard applied to time, place, or manner restrictions." (citation and quotation marks omitted)).

The Act is a valid exercise of Congress's power over foreign affairs and national security. The Court should dismiss the Petition.

## ARGUMENT

### I. TikTok is a threat to national security and consumer privacy.

#### A. Extensive public reporting shows that TikTok's U.S. user data is subject to at-will Chinese Communist Party access.

Over the last three years, a tidal wave of government reports and news stories revealed how TikTok harms Americans.[3] "[L]eaked audio from more than 80 internal TikTok meetings" established that ByteDance employees based in China "have repeatedly accessed

[3] *See, e.g.*, *TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms, House Energy & Commerce*, 118th Cong. (Mar. 23, 2023), perma.cc/JTE9-5GLK; *Deputy attorney general warns against using TikTok, citing data privacy*, ABCNEWS (Feb. 16, 2023), perma.cc/GKK7-BX9D; David Shepardson, *State AGs demand TikTok comply with US consumer protection investigations*, REUTERS (Mar. 6, 2023), perma.cc/9NL6-2VPW.

nonpublic data about US TikTok users."[4] Statements from TikTok employees and directors reveal that "'[e]verything is seen in China,'" and "one Beijing-based engineer" acts "as a 'Master Admin' who 'has access to everything.'" *Id.* One report found that "[w]hen TikTok users enter a website through a link on the app, TikTok inserts code that can monitor much of their activity on those outside websites, including their keystrokes and whatever they tap on the page"—so "TikTok [could] capture a user's credit card information or password."[5] The researcher who discovered that code described this code injection as "'a non-trivial engineering task'" that "'does not happen by mistake.'" *Id.* In 2022, two articles reported how ByteDance accessed TikTok user data from two U.S. journalists to try to identify the source of a leak of internal TikTok information.[6]

---

[4] Emily Baker-White, *Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEEDNEWS (June 17, 2022), perma.cc/LAM2-PL6K.

[5] Richard Nieva, *TikTok's In-App Browser Includes Code That Can Monitor Your Keystrokes, Researcher Says*, FORBES (Aug. 18, 2022), perma.cc/M578-4X29.

[6] Emily Baker-White, *Exclusive: TikTok Spied on Forbes Journalists*, FORBES (Dec. 22, 2022), perma.cc/8HSX-R74Q; David Shepardson, *ByteDance finds employees obtained TikTok user data of two journalists*, REUTERS (Dec. 22, 2022), perma.cc/YH2U-RLA8.

In March 2023, a whistleblower told a U.S. Senator that "TikTok's access controls on U.S. user data are much weaker than the company says" and that "TikTok overstates its separation from its China-based owner ByteDance, relies on proprietary Chinese software that could have backdoors, and uses tools that allow employees to easily toggle between U.S. and Chinese user data."[7] A second whistleblower told congressional investigators and the *Washington Post* that TikTok's "plan for protecting United States user data is deeply flawed," that "issues could leave data from TikTok's more than 100 million U.S. users exposed to China-based employees of its parent company ByteDance," and "that a truly leakproof arrangement for Americans' data would require a 'complete re-engineering' of how TikTok is run."[8]

Two months later, the former head of engineering for ByteDance in the U.S. sued ByteDance, alleging that "ByteDance offices in Beijing had a special unit of Chinese Communist Party members sometimes referred

[7] Ashley Gold, *Exclusive: Senator's TikTok whistleblower alleges data abuses*, AXIOS (Mar. 8, 2023), https://www.axios.com/2023/03/08/senators-tiktok-whistleblower-alleges-data-abuses.

[8] Drew Harwell, *A former TikTok employee tells Congress the app is lying Chinese spying*, WASH. POST (Mar. 10, 2023), perma.cc/997H-9GLY.

to as the Committee," which "'maintained supreme access to all the company data, even data stored in the United States.'"[9] Indeed, "[d]uring his tenure at the company, he said, certain engineers had 'backdoor' access to user data." *Id.*

A few weeks later, the *New York Times* reported on TikTok's "internal messaging and collaboration tool called Lark."[10] Lark is a tool "used every day by thousands of employees of the app's Chinese owner, ByteDance, including by those in China," that "has been used for handling individual TikTok account issues and sharing documents that contain personally identifiable information since at least 2019." *Id.*

Most recently, the former ByteDance executive alleged that "some members of the ruling Communist Party" had "access to U.S. user data" through a "'superuser' credential, also known as a god credential.[11] This

---

[9] Thomas Fuller & Sapna Maheshwari, *Ex-ByteDance Executive Accuses Company of "Lawlessness*," N.Y. TIMES (May 12, 2023), perma.cc/DE96-KD7G.

[10] Sapna Maheshwari & Ryan Mac, *Driver's Licenses, Addresses, Photos: Inside How TikTok Shares User Data*, N.Y. TIMES (May 24, 2023), perma.cc/2KBM-WSAZ.

[11] Zen Soo, *Former exec at TikTok's parent company says Communist Party members had a 'god credential' that let them access Americans' data*, BUSINESS INSIDER (June 7, 2023), perma.cc/5QXY-5GBE.

credential enabled a special committee of Chinese Communist Party members stationed at the company to view all data collected by ByteDance including those of U.S. users." *Id.* He alleged that "[t]he credential acted as a 'backdoor to any barrier ByteDance had supposedly installed to protected data from the CCP's surveillance." *Id.*

TikTok concedes that it is owned by ByteDance, Ltd., a shell corporation registered in the Cayman Islands. Congressional testimony establishes other key facts (unrebutted by TikTok) concerning TikTok's ownership. First, ByteDance's key subsidiary in China is called Beijing ByteDance Technology, and the Chinese government owns a 1% stake in that subsidiary yet has installed a director on its Board.[12] Second, according to ByteDance's Cayman corporate registry, the director in charge of the shell corporation is also listed as the CEO of the ByteDance corporation registered under Chinese Law. *Id.* at 6. Third, under Chinese law, the Chinese Communist Party can force ByteDance to turn over TikTok's U.S. user data and manipulate content displayed on the app. *See id.* at

[12] *Hearing on Social Media's Impact on Homeland Security Before the H.R. Comm. on Homeland Sec. & Governmental Affs.*, 117th Cong. (Sept. 14, 2022) (written testimony of Geoffrey Cain, Senior Fellow for Critical Emerging Techs., Lincoln Network), at 7, https://perma.cc/L3V6-MKE8.

7-8. Fourth, the lack of transparency from ByteDance makes it difficult to determine whether such a request has taken place. *See id.* at 7.

These revelations reflect "the reality that Chinese companies are subject to the whims of the authoritarian Chinese Communist Party," raising the "risk" that the Chinese "government could force ByteDance to collect and turn over information" on Americans "as a form of 'data espionage.'" *Leaked Audio*, *supra* n.6. That risk is not speculative; the head of Canada's intelligence agency has warned that "there is a very clear strategy on the part of the government of China ... to be able to acquire ... personal information from anyone around the world."[13] Further, it's "very clear" from TikTok's design that data gleaned from its users "is available to the government of China." *Id.* And the Secretary of Commerce designated the People's Republic of China a "foreign adversary" after determining that China has "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons." 15 C.F.R. §7.4(a)(1).

[13] Catharine Tunney, *Intelligence chief warns Canadians that China can use TikTok to spy on them*, CBC NEWS (May 17, 2024), https://perma.cc/C5ZH-QRE7.

And TikTok's troubles continue. In February 2024, a different former TikTok executive sued over age- and gender-based discrimination.[14] The former executive alleges that after Shou Chew took over as TikTok's chief executive in May 2021, "control of at least one key department"—the Global Business Solutions team—"remained with ByteDance leadership." Duffy, *supra* n.14. That unit, which the former executive was a part of, controlled TikTok ad revenues and ad placements, and it "continued to report up to a senior ByteDance executive in China." *Id.*

Around the same time, a bipartisan group of lawmakers urged Commerce Secretary Gina Raimondo to add ByteDance to the Bureau of Industry Security's Entity List, which restricts U.S. exports of goods, software, and technology to the listed entities.[15] The lawmakers highlighted the "serious issues with access to U.S. user data, and the

---

[14] Clare Duffy, *Former TikTok executive sues the company for alleged gender and age discrimination*, CNN BUSINESS (Feb. 9, 2024), https://perma.cc/PKP3-RPYJ; *see also Purris v. TikTok Inc*, No. 1:24-cv-00944 (S.D.N.Y. Feb. 8, 2024), ECF No. 1, ¶ 20 ("Despite its attempts to appear independent, TikTok's day-to-day management and business decisions came directly from ByteDance's top-level management in China.").

[15] Zach Kessel, *Crenshaw, Gottheimer Urge Commerce Department to Block TikTok from Transferring U.S. Data to CCP-Linked Parent Company*, NAT'L REV. (Feb. 8, 2024), https://perma.cc/AU82-U45P.

relationship between ByteDance and the Chinese Communist Party," adding that "TikTok's software engineering personnel ultimately report to ByteDance leadership in the People's Republic of China." *Id.*

Even TikTok's alleged fix to its data security concerns—the so-called "Project Texas"—has been plagued with credible allegations of fraud and Chinese Communist Party influence. *See* Harwell, *supra* n.8. Project Texas was allegedly TikTok's attempt to silo off its U.S. operations from ByteDance. But where TikTok stores data is "irrelevant" to ByteDance's ability to access the data.[16] Former employees say that Project Texas was "largely cosmetic" and that they continued to work closely with Beijing-based ByteDance executives after the plan's implementation.[17]

For example, a data scientist described a "stealth chain of command" in which he was reassigned—on paper—to a manager in Seattle but continued reporting to executives in China. He would email

---

[16] D. Harwell & T. Room, *Inside TikTok: A culture class where U.S. views about censorship often were overridden by the Chinese bosses*, Washington Post (Nov. 5, 2019), http://tinyurl.com/mr28su7n.

[17] Alexandra Sternlicht, *Some ex-TikTok employees say the social media service worked closely with its China-based parent despite claims of independence*, FORTUNE (Apr. 15, 2024).

spreadsheets with data on hundreds of thousands of U.S. users to ByteDance workers in Beijing. *Id.* The spreadsheets were used to determine how to develop TikTok's algorithm to encourage users to be more active on the app, and they included users' names, email addresses, IP addresses, and geographic and demographic information. *Id.* Earlier this year, the *Wall Steet Journal* reported that managers have instructed U.S.-based workers to share data with colleagues elsewhere in the company—including with ByteDance employees.[18]

And that's just the publicly available information.[19] But despite this mountain of evidence, TikTok told a federal district court in Montana that these concerns were "based entirely on unfounded speculation." Br. in Supp. of Consol. Pls' Mot. for Prelim. Inj. ("TikTok P.I. Br."), *Alario, et al. v. Knudsen*, 9:23-cv-56 (D. Mont. July 5, 2023), ECF No. 12, at 28. It is not; TikTok is a threat to data privacy and national security.

[18] Georgia Wells, *TikTok Struggles to Protect U.S. Data From Its China Parent*, WALL ST. J. (Jan. 30, 2024).

[19] TikTok's pattern of deception also suggests the Court should give little, if any, weight to the opinions of TikTok's putative expert, Dr. Webber.

### B. States have taken action to protect consumers from Chinese Communist party threats.

States have acted to protect their citizens from the privacy threat that TikTok poses. Data harvesting is one of the most acute modern threats to citizens' privacy.[20] It has become nearly ubiquitous, and with its ubiquity have also come corresponding risks of the misuse of data. The more that any user's data is "passed around between countless third parties," the more possibilities there are for that user's data to be "leaked or breached in a way that causes real harm" or to be "used in surprising ways … such as in targeting ads or adjusting interest rates based on race." *Id.*

Over eight billion accounts were targeted in data breaches in 2023, with over 2,800 data breaches and cyber attacks recorded.[21] That flood continued in 2024, with 26 billion account records having been stolen just

---

[20] T. Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://tinyurl.com/ms6cv842.

[21] N. Ford, *List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached*, IT GOV. BLOG (Jan. 5, 2024), http://tinyurl.com/43wv66ah.

a few months ago in the "mother of all breaches."[22] Even large and sophisticated businesses are not immune. For instance, in October 2023, hackers stole the ancestry data of almost seven million of 23andMe's customers, apparently targeting users of Ashkenazi Jewish descent.[23]

Recognizing this threat, states stepped in to safeguard their citizens' personal data. More than a dozen states have enacted comprehensive privacy laws. These privacy laws typically prohibit businesses from "process[ing] personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent." *See, e.g.*, Va. Code §59.1-578(A)(2).

But even with these safeguards, TikTok is a unique threat to American consumers. TikTok not only collects large amounts of its users' personal data, but also shares that data with the Chinese Communist Party

---

[22] B. Kato, *'Mother of all breaches' data leak reveals 26 billion account records stolen from Twitter, LinkedIn, more*, N.Y. POST (Jan. 23, 2024), http://tinyurl.com/dk97hj2m.

[23] L. Franceschi-Bicchierai, *23andMe confirms hackers stole ancestry data on 6.9 million users*, TECHCRUNCH (Dec. 4, 2023), http://tinyurl.com/2thwyhy5.

because its parent company is a Chinese company subject to Chinese laws. *See supra* nn. 2-23. Thus, states have taken steps to hold TikTok accountable for harm to consumers. Since March 2022, TikTok has faced a 47-state investigation from state attorneys general regarding its alleged practice of inducing children to use its social media platform, resulting in harm to minors. Some states have even investigated or sued TikTok for misleading consumers about its data practices and ties to China.[24]

But TikTok's obstinance and failure to preserve records properly have stymied these efforts. In March 2023, 46 states explained to a Tennessee court how TikTok's failure to preserve potentially relevant evidence and failure to produce information in a reasonably useful format had hampered investigations across the country.[25] In December 2023, a North Carolina court granted a motion to compel after the state's

[24] *See, e.g.*, Lauren Feiner, *Utah accuses TikTok of misleading users about safety, China connection in new lawsuit*, CNBC (Oct. 10, 2023), https://perma.cc/PTU8-JKGC.

[25] Mot. Leave Br. Amicus Curiae Colo. Dep't of Law and 45 Other States, *In re: Investigation of TikTok, Inc.*, No. 23-0298-IV (Tenn. Ch. Ct. Mar. 6, 2023), https://coag.gov/app/uploads/2023/03/2023.03.06-Motion-for-Leave-for-Brief-of-Amici-Curiae1794146.1.pdf

investigation discovered that TikTok had a secret archive of tens of thousands of recorded internal Zoom meetings that it failed to disclose for nearly a year and a half.[26] Indeed, TikTok's own internal audit and risk control team said it could not ensure accurate responses to government inquiries.[27]

In 2023, the Montana Legislature acted decisively to protect its citizens with SB 419, which banned TikTok from operating in the state unless it divested itself of Chinese Communist Party ties. TikTok sued in federal district court. Even though Montana's concerns were rooted in data security and consumer privacy, TikTok argued that federal law preempted SB 419. According to TikTok, although Montana could enact generic data privacy laws to protect consumers, it was powerless to address the unique threat of Chinese spying via TikTok because it implicated foreign affairs and national security, over which the federal government has exclusive authority. TikTok P.I.Br.28. TikTok highlighted

---

[26] Att'y Gen. Josh Stein, *Court Orders TikTok to Comply with Attorney General Josh Stein's Investigation*, NCDOJ (Dec. 15, 2023), https://perma.cc/26H8-9RRK.

[27] Emily Baker-White, *TikTok Couldn't Ensure Accurate Responses to Government Inquiries, A ByteDance Risk Assessment Said*, FORBES (Nov. 28, 2022), https://perma.cc/526H-XSSX.

several federal statutes that, TikTok argued, address the purported national security risks in SB 419 and left "no room for state regulation." *Id.* at 29. In support of preemption, TikTok (ironically) cited the ongoing negotiations between TikTok and the Committee on Foreign Investment in the United States under 721 of the Defense Production Act. *Id.* So, despite TikTok claiming that Montana's law was based on "unfounded speculation" regarding its data security practices and Chinese Communist Party ties, its case for preemption centered around its negotiations with the federal government over national security concerns.

But TikTok's arguments in this case demonstrate that it is trying to have its cake and eat it too. In the Montana litigation, TikTok claims that only Congress can address the unique data security concerns from its association with the Chinese Communist Party. But in this case, TikTok argues that Congress is powerless to force the divestiture. In other words, TikTok asks this Court to declare that the peoples' representatives are powerless at all levels of government to stop a hostile foreign power from spying on Americans. TikTok and the Chinese Communist Party cannot hide behind the First Amendment.

## II. TikTok is unlikely to succeed on the merits of its First Amendment claim.

### A. The Act doesn't implicate First Amendment rights.

A statute only triggers First Amendment scrutiny if it targets "conduct with a significant expressive element" or, if "based on a nonexpressive activity," it "has the inevitable effect of singling out those engaged in expressive activity." *Arcara*, 478 U.S. at 706-07; *see also Talk of the Town v. Dep't of Fin. & Bus. Servs.*, 343 F.3d 1063, 1069 (9th Cir. 2003). The Act does neither. It does not, as TikTok claims, "restrict expression because of its message, its ideas, its subject matter, or its content." *Police Dep't of Chi. v. Mosley*, 408 U.S. 92, 95 (1972). Rather, the Act restricts TikTok's operation to protect Americans' data privacy from a hostile foreign power.

TikTok's arguments rest on a "fallacy" the Supreme Court has rejected: "seeking to use the First Amendment as a cloak for obviously unlawful … conduct by … attributing protected expressive attributes to that conduct." *Arcara*, 478 U.S. at 705. In *Arcara*, an adult bookstore became a site of prostitution and other public sex acts. The Court concluded that the First Amendment's protection for selling books didn't shield the bookstore from liability for violating prostitution laws: "the

First Amendment is not implicated by the enforcement of a public health regulation of general application against the physical premises in which respondents happen to sell books." *Id.* at 707. That is, the First Amendment "has no relevance to a statute directed at imposing sanctions on nonexpressive activity," and "[b]ookselling in an establishment used for prostitution does not confer First Amendment coverage to defeat a valid statute aimed at penalizing and terminating illegal uses of premises." *Id.*; *see also Talk of the Town,* 343 F.3d at 1069.

Like the statutes in *Arcara*, the Act bans TikTok not for its speech but because of separate harms: its practices of harvesting reams of personal, private data from American users and sharing that data with a hostile foreign government. *See supra* nn.3-23. No other platform conditions its use on making Americans' digital privacy subject to data harvesting with at-will Chinese Communist Party access. There are no protected expressive attributes in a hostile foreign government's massive data-harvesting efforts intentionally directed at Americans. *Arcara*, 478 U.S. at 707. That is true even though TikTok harvests Americans' data while transmitting expressive videos to them. Just as books did not transform prostitution into expressive conduct in *Arcara*, TikTok's short-

form videos "do[] not confer First Amendment coverage to defeat a valid statute aimed at" protecting Americans from forced data-harvesting subject to at-will Chinese Communist Party access. *Id.*

Were it otherwise, Congress would be powerless to ban a cancer-causing radio merely because that radio also transmitted protected speech, or to ban sports-betting apps merely because those apps also shared informative videos teaching their users the intricacies of sports gambling. The targeted harms—preventing cancer, illegal gambling, or data-gathering by a hostile foreign state—are inherently nonexpressive. Overlaying them with expressive conduct—radio communications or instructive videos—does not change that calculus. *See id.* at 705-07.

To the extent this Court considers out-of-circuit district court cases, the Montana District Court's preliminary-injunction decision regarding the Montana legislation in *Alario* should be of little persuasive value. *See Alario v. Knudsen*, 2023 U.S. Dist. LEXIS 213547 (D. Mont. Nov. 30, 2023). *Alario* distinguished *Arcara* on two grounds, but both distinctions fail. First, it thought *Arcara* inapposite because the law "implicates traditional First Amendment speech." *Id.* at *16. Second, it concluded that,

unlike the public nuisance statute in *Arcara*, the law targeted a single entity—TikTok—and thus isn't generally applicable.

The first distinction fails because the relevant inquiry is not whether the law "implicates traditional First Amendment speech," but whether it targets "conduct with a significant expressive element." *See Arcara*, 478 U.S. at 706. The Act here targets a hostile foreign government's data-harvesting efforts intentionally directed at Americans. As explained above, that is nonexpressive conduct, even if TikTok harvests Americans' data while transmitting expressive videos to them. TikTok cannot use the First Amendment "as a cloak" for its data-harvesting practices by "attributing protective expressive attributes to that conduct." *Id.* at 705, 707.

The second distinction likewise fails because a regulation—even one targeted at specific entities—"does not implicate the First Amendment" unless it "is directed at, or presents the danger of suppressing, particular ideas." *Leathers v. Medlock*, 499 U.S. 439, 453 (1991); *see also Turner Broad. Sys. v. FCC*, 512 U.S. 622, 660-61 (1994) ("heightened scrutiny is unwarranted when the differential treatment is justified by some special characteristic of the particular medium being regulated"

(internal quotations omitted)). The Act singles out TikTok not because of its ideas or viewpoints, but because of its unique data harvesting practices and ties to a hostile foreign power.

To be sure, some cases emphasize that the public nuisance statute in *Arcara* was generally applicable. *E.g.*, *Wright v. City of St. Petersburg*, 833 F.3d 1291, 1296-97 (11th Cir. 2016); *Doe v. Harris*, 772 F.3d 563, 572-73 (9th Cir. 2014). But *Arcara* considered general applicability to determine whether a statutory distinction was "drawn … [to] single out [those] engaged in First Amendment protected activities for the imposition of its burden,"[28] *see* 478 U.S. at 705—that is, whether the statute's operation warrants an inference that suppression of speech was the statute's real aim. *See Turner Broad.*, 512 U.S. at 660 (explaining that in the tax cases—*Minnesota Star* and *Arkansas Writers Project*—the structure of

[28] Even though they note that *Arcara* involved a generally applicable statute, *Wright* and *Doe* both focus on whether the statute targets speech for suppression. *Wright*, 833 F.3d at 1297 (observing that the challenged ordinance didn't have the inevitable effect of singling out anyone engaged in expressive activity); *Doe*, 772 F.3d at 573 ("[T]he CASE Act directly and exclusively burdens speech, and a substantial amount of that speech is clearly protected under the First Amendment." (emphasis added)). Thus, *Wright* and *Doe* suggest that general applicability serves as a proxy for determining whether a facially neutral statute really intends to suppress speech.

the regulation "raised suspicions that [the government] objective was, in fact, the suppression of certain ideas"). There is no such aim here. The concerns animating the Act—concerns shared across the political spectrum, across state and federal government agencies and legislatures, across state lines, and across the pond—are TikTok's data-harvesting practices and ties to the Chinese Communist Party.

### B. If the Act implicates First Amendment rights, it passes scrutiny under *O'Brien*.

Even if the Act implicates the First Amendment, the Supreme Court has rejected the view that all conduct is protected if a person "intends thereby to express an idea." *O'Brien*, 391 U.S. at 376.[29] If regulated nonspeech conduct also contains a speech element, the Court applies a four-part test to assess the law's constitutionality. *Id.* at 377. That test considers whether the government regulation (1) "is within the

[29] The district court in *Alario* erroneously disputed *O'Brien*'s application, relying on *Boy Scouts of Am. v. Dale*, 530 U.S. 640, 659 (2000), which it claimed holds that when a law "'directly and immediately affects' First Amendment rights, '*O'Brien* is inapplicable.'" *Alario*, 2023 U.S. Dist. LEXIS 213547, at *20. But the Act here targets TikTok's conduct, not its expression. That it happens to burden TikTok's expression, and any burden on TikTok's expression is "incidental." *O'Brien*, 391 U.S. at 377. So if First Amendment scrutiny is required at all, *O'Brien* applies.

[government's] constitutional power"; (2) "furthers an important or substantial governmental interest" that is (3) "unrelated to the suppression of free expression"; and (4) burdens "alleged First Amendment freedoms … no greater than is essential to the furtherance of that interest." *Id.* The Act satisfies this standard.

As to the first two elements, the Act's national security and foreign affairs rationale falls within Congress's "constitutional authority" and furthers its "substantial interests" in protecting Americans from hostile foreign powers. U.S. Const. Art. I § 8; *see Ziglar v. Abbasi*, 582 U.S. 120, 142 (2017) ("National-security policy is the prerogative of the Congress and President"); *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948 (D.C. Cir. 2024) ("We cannot second-guess the FCC's judgment that allowing China to access this information poses a threat to national security. That deference is redoubled by the repeated acts of Congress expressly identifying TikTok's video-surveillance equipment as posing national-security risks.").

As to the third element, the national security interest here is "unrelated to the suppression of free expression." *O'Brien*, 391 U.S. at 377. The Act prohibits using TikTok regardless of the messages it conveys, or

the fact that it conveys messages at all. Rather, the "perceived evil" the Act targets is TikTok's data harvesting with at-will access for the Chinese Communist Party—harms that would justify regulating TikTok regardless of whether it expressed anything whatsoever. *Barnes v. Glen Theatre*, 501 U.S. 560, 571 (1991); *Masterpiece Cakeshop, Ltd. v. Colo. Civ. Rts. Comm'n*, 584 U.S. 617, 664 (2018) (Thomas, J., concurring in part and concurring in the judgment) (*O'Brien* applies if "the [State] would have punished the [nonexpressive] conduct regardless of its expressive component.").

On the final element, the Act's restrictions are "no greater than is essential" to furthering Congress's interest in protecting Americans' data privacy. *O'Brien*, 391 U.S. at 377. The Act "need not be the least restrictive or least intrusive means of" furthering that interest to survive intermediate scrutiny. *See Ward*, 491 U.S. at 797-98. For example, applying that standard, the Ninth Circuit rejected a claim that mandatory school uniforms violated intermediate scrutiny because they limited students' self-expression through clothing choices, holding that the students retained "'ample alternative channels' for student communication." *Jacobs v. Clark Cnty. Sch. Dist.*, 526 F.3d 419, 437 (9th Cir. 2008). Even though

that policy limited expression, students could "'express themselves through other and traditional methods of communication throughout the school day,'" including through "verbal conversations with other students, publish[ing] articles in school newspapers, and join[ing] student clubs." *Id*.

The Act survives intermediate scrutiny for the same reason. Like the school's uniform policy, the Act limits Americans' abilities to express themselves on TikTok, but they "may continue to express themselves through other and traditional methods of communication" by sharing videos, memes, and *every other* kind of expressive content on *every other* internet-based video or social-media platform. *Jacobs*, 526 F.3d at 437. Indeed, the Act is less restrictive than the uniform policy in *Jacobs* because the Act does not affect any other app or part of the internet. Thus, the Act is "not a means to some greater end" that targets expression "but an end in itself." *Barnes*, 501 U.S. at 572.

### C. The Act is neither a content- nor viewpoint-based restriction on speech.

TikTok attacks the Act as a content- and viewpoint-based speech restriction. Those claims fail. The "content-based" inquiry first asks whether the regulation is "content neutral on its face." *Reed v. Town of*

*Gilbert*, 576 U.S. 155, 165 (2015). If so, the pertinent question "is whether the government has adopted a regulation of speech *because* of disagreement with the message it conveys." *Ward*, 491 U.S. at 791 (emphasis added). Any such regulations are subject to strict scrutiny. *Reed*, 576 U.S. at 165. But "a regulation that serves purposes unrelated to the content of expression is deemed neutral," *Ward*, 491 U.S. at 791, and need only satisfy intermediate scrutiny, *Turner Broad.*, 512 U.S. at 642.

The Act "regulate[s] the manner—not the content—of affected speech." *Lone Star Sec. & Video, Inc. v. City of L.A.*, 827 F.3d 1192, 1200 (9th Cir. 2016). And it applies equally to all speech on the platform. *Id.* It does not prohibit TikTok "based on the type of information" it conveys, *Reed*, 576 U.S. at 159, nor does it distinguish "between commercial and noncommercial forms of expression," *S.O.C., Inc. v. Cnty. of Clark*, 152 F.3d 1136, 1145 (9th Cir. 1998). "There has been no suggestion that [the Act] appl[ies] differently to … political endorsements than to its commercial promotional campaigns." *Lone Star*, 827 F.3d at 1200. Nor does the Act prohibit only videos showing certain conduct, ; it applies to the platform writ large. *Foti v. City of Menlo Park*, 146 F.3d 629, 635-36 (9th Cir. 1998). It is a content-neutral regulation.

TikTok's viewpoint-discrimination claim fails for the same reasons. Nothing in the Act regulates use of TikTok "because of disagreement with the message," *Ward*, 491 U.S. at 791, or disagreement with "particular views taken" on a subject, *Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 829 (1995). The Act regulates all content, viewpoints, and speakers equally. *Cf. id.* at 836-37 (declaring unconstitutional the withholding of funding for a student newspaper because it "promote[d] or manifest[ed] a particular belief in or about a deity or ultimate reality") (cleaned up); *R.A.V. v. St. Paul*, 505 U.S. 377, 390 (1992) (declaring unconstitutional a law prohibiting fighting words containing bias-motivated hatred); *Lamb's Chapel v. Ctr. Moriches Union Free Sch. Dist.*, 508 U.S. 384, 393 (1993) (declaring unconstitutional a policy permitting presentations "about family issues and child rearing except those dealing with the subject matter from a religious standpoint"). The Act permits any person to make any statement about any topic, even China. It just prohibits the use of TikTok unless the Chinese parent company divests its U.S. operations. *See Leathers*, 499 U.S. at 444 (that one medium "is taxed differently from other media does not by itself, however, raise First Amendment concerns").

Thus, even if the Act regulated speech by barring TikTok's operation (it does not), intermediate scrutiny would apply because the Act applies to all speech on TikTok no matter its substance or message. *Perry Educ. Ass'n v. Perry Loc. Educators' Ass'n*, 460 U.S. 37, 45 (1983). The government need only show that the Act furthers a substantial or important government interest unrelated to the suppression of expression, and that the "incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *Jacobs*, 526 F.3d at 434 (quoting *Turner Broad.*, 512 U.S. at 661-62). The Act does both.

Courts begin by evaluating whether "*the government's stated goals* [for the policy] qualify as important or substantial." *Jacobs*, 526 F.3d at 435. As discussed above, Congress has a substantial and important interest in its national security unrelated to expression. The Act reflects widespread concern over TikTok's data-privacy practices. *See supra* nn. 3-23.

The Act is narrowly drawn. It does not ban all online platforms that enable users to create, share, and view videos and other forms of content. Rather, it "eliminate[d] the exact source of the evil it sought to

remedy." *Members of the City Council of the City of L.A. v. Taxpayers for Vincent,* 466 U.S. 789, 808 (1984). The Act is like the school-uniform policy in *Jacobs*—it regulates one channel of expression but leaves all others untouched. Unlike cases in which the speakers' preferred medium was banned entirely, the Act does not impose a blanket prohibition on creating, sharing, and viewing videos on *every* internet-based application. *Cf. Schad v. Borough of Mount Ephraim*, 452 U.S. 61, 75 (1981) (all live entertainment); *Martin v. City of Struthers*, 319 U.S. 141, 142 (1943) (all door-to-door distribution of literature); *City of Ladue v. Gilleo*, 512 U.S. 43, 56 (1994) (all residential yard signs). Rather, it responds to the unique threat that TikTok poses by sharing Americans' personal data with a hostile foreign power. Amici States are grateful that Congress acted to protect the American people. The Act is fully consistent with the First Amendment.

## CONCLUSION

This Court should declare that the Act is constitutional and dismiss the Petition.

Respectfully submitted this 2nd day of August, 2024.

AUSTIN KNUDSEN
*Attorney General of Montana*
CHRISTIAN B. CORRIGAN
*Solicitor General*

*/s/ Peter M. Torstensen, Jr.*
PETER M. TORSTENSEN, JR.
*Deputy Solicitor General*
MONTANA DEPARTMENT OF JUSTICE
215 North Sanders
P.O. Box 201401
Helena, MT 59620-1401
(406) 444.2026
peter.torstensen@mt.gov

*Counsel for State of Montana*

JASON S. MIYARES
*Attorney General of Virginia*
ERIKA L. MALEY
*Solicitor General*

*/s/ Kevin M. Gallagher*
KEVIN M. GALLAGHER
*Principal Deputy Solicitor General*
MICHAEL DINGMAN
*Assistant Solicitor General*
OFFICE OF THE ATTORNEY GENERAL
202 North Ninth Street
Richmond, VA 23219
(406) 786-2071
KGallagher@oag.state.va.gov

*Counsel for State of Virginia*

## ADDITIONAL COUNSEL

Steve Marshall
ALABAMA ATTORNEY GENERAL

Treg Taylor
ALAKSA ATTORNEY GENERAL

Tim Griffin
ARKANSAS ATTORNEY GENERAL

Ashley Moody
FLORIDA ATTORNEY GENERAL

Christopher M. Carr
GEORGIA ATTORNEY GENERAL

Raúl R. Labrador
IDAHO ATTORNEY GENERAL

Theodore E. Rokita
INDIANA ATTORNEY GENERAL

Brenna Bird
IOWA ATTORNEY GENERAL

Russell Coleman
KENTUCKY ATTORNEY GENERAL

Liz Murrill
LOUISIANA ATTORNEY GENERAL

Lynn Fitch
MISSISSIPPI ATTORNEY GENERAL

Andrew Bailey
MISSOURI ATTORNEY GENERAL

Michael T. Hilgers
NEBRASKA ATTORNEY GENERAL

John M. Formella
NEW HAMPSHIRE ATTORNEY GENERAL

Gentner F. Drummond
OKLAHOMA ATTORNEY GENERAL

Alan Wilson
SOUTH CAROLINA ATTORNEY GENERAL

Marty J. Jackley
SOUTH DAKOTA ATTORNEY GENERAL

Jonathan Skrmetti
TENNESSEE ATTORNEY GENERAL AND REPORTER

Sean D. Reyes
UTAH ATTORNEY GENERAL

## CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(g) of the Federal Rules of Appellate Procedure, Peter M. Torstensen, Jr., an employee in the Office of the Attorney General of the Montana, hereby certifies that according to the word count feature of the word processing program used to prepare this brief, the brief contains 6,123 words, excluding the parts of the document exempted by Rule 32(f), and complies with the typeface requirements and length limits of Rules 29 and 32(a)(5)-(7) and corresponding local rules.

*/s/ Peter M. Torstensen, Jr.*
PETER M. TORSTENSEN, JR.