ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024

United States Court of Appeals for the District of Columbia Circuit

No. 24-1113

(and Consolidated Cases 24-1130 & 24-1183)

TIKTOK INC. and BYTEDANCE LTD.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

(For Continuation of Caption See Inside Cover)

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

BRIEF OF *AMICI CURIAE* ZEPHYR TEACHOUT, MARK MEADOR, MATTHEW STOLLER, AND JOEL THAYER IN SUPPORT OF RESPONDENT

JOEL L. THAYER
THAYER, PLLC
1255 Union Street, 7th Floor
Washington, D.C. 20002
jthayer@thayer.tech
(760) 668-0934

Counsel for Amici Curiae

August 2, 2024

CP COUNSEL PRESS (800) 4-APPEAL • (331583)

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.

CIRCUIT RULE 29(D) STATEMENT

Amici certify they are not aware of any other amicus brief addressing the subject of this brief—in particular, representing academics that can speak directly to the legal and policy history of foreign ownership restrictions and how the U.S. has traditionally applied them to communications systems. A separate brief is necessary to permit *amici* joining this brief to offer their perspectives on their unique issues before the Court.

CERTIFICATE AS TO PARTIES, RULINGS UNDER REVIEW, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), amici certify as follows:

(A) Parties and Amici.

The parties to *TikTok Inc. v. Garland*, No. 24-1113, are petitioners TikTok Inc. and ByteDance Ltd. ("TikTok Petitioners") and respondent Merrick B. Garland, in his official capacity as Attorney General of the United States. The parties to the first consolidated case, *Firebaugh v. Garland*, No. 24-1130, are petitioners Brian Firebaugh, Chloe Joy Sexton, Talia Cadet, Timothy Martin, Kiera Spann, Paul Tran, Christopher Townsend, and Steven King ("Creator Petitioners") and respondent Merrick B. Garland, in his official capacity as Attorney General of the United States. The parties to the second consolidated case, BASED Politics Inc. v. Garland, No. 24-1183, are petitioner BASED Politics Inc. and respondent

Merrick B. Garland, in his official capacity as Attorney General of the United States.

Aside from the parties above, and any amicus briefs filed prior to and after this one, amici include: Zephyr Teachout, Mark Meador, Matthew Stoller, and Joel Thayer.

(B) Orders Under Review.

Petitioners seek direct review of the constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications (the "Act) H.R. 815, div. H, 118th Cong., Pub. L. 118-50 (Apr. 24, 2024), such that there are no prior rulings under review.

(C) Related Cases.

To the best of amici's knowledge, there are no related cases within the meaning of Circuit Rule 28(a)(1)(C).

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and D.C. Circuit Rule 26.1, amici state that they have no parent corporations and that no publicly held company owns ten percent (10%) or more of any amici's organizations.

STATEMENT OF AUTHORSHIP AND FINANCIAL CONTRIBUTIONS

Amici certify that no party or party's counsel authored this brief in whole or in part, that no party or party's counsel provided any money intended to fund the preparation or submission of this brief, and no party or person—other than amici's counsel—contributed money intended to fund the preparation or submission of this brief.

CONSENT TO FILE

This brief is being filed on consent of the parties.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes & Other Authorities:

IDENTITY OF *AMICI*, INTEREST IN THIS MATTER, AND SOURCE OF AUTHORITY TO FILE

Pursuant to Fed. R. App. P. 29(a), Zephyr Teachout, Mark Meador, Matthew Stoller, and Joel Thayer represent that they seek to participate as amici curiae in support the Protecting Americans from Foreign Adversary Controlled Applications Act.

Zephyr Teachout is a Professor at Law at Fordham Law School where she focuses on the intersection of corporate power and political power. She teaches corporations, election law, antitrust, and prosecuting white collar crime. Teachout's most recent book, Break 'em Up (2020), makes a case for reimagining the relationship between democracy and antimonopoly law. Her prior book, Corruption in America (2014), argued that the American constitutional system has an embedded anti-corruption principle that has been discarded by the modern Court. Her public writings have appeared in the New York Times, Foreign Affairs, New York Review of Books, Washington Post, The Nation and The New Republic. Teachout has helped draft state and federal antitrust reform bills and child social media laws, and in 2010 wrote the first law review article warning of how new technologies could threaten domestic sovereignty and peace by enabling foreign intervention in domestic elections.

Mark Meador is a visiting fellow at the Heritage Institute's Tech Policy Center. He has extensive experience in antitrust enforcement from his previous

roles at the Federal Trade Commission and the Department of Justice Antitrust Division. He also worked as a competition policy expert on Capitol Hill and continues to be a leading voice on competition policy as a partner at the boutique antitrust law firm Kressin Meador LLC. Meador served as deputy chief counsel for antitrust and competition policy for U.S. Sen. Mike Lee, ranking member on the Senate Judiciary Antitrust Subcommittee. In this role, Meador helped shape critical antitrust reform bills and provided expert guidance to advance the senator's goal of holding Big Tech accountable to the American people. Prior to his time in the Senate and the Department of Justice, Meador was also an associate in private practice at Paul, Weiss, Rifkind, Wharton & Garrison LLP.

Matthew Stoller is a public intellectual who writes about the American anti-monopoly tradition. He is the author of the Simon and Schuster book Goliath: The Hundred Year War Between Monopoly Power and Democracy. Stoller is the Director of Research at the American Economic Liberties Project. He publishes an email newsletter called BIG. Stoller is a former policy advisor to the Senate Budget Committee, and worked in the House of Representatives on the Dodd–Frank Wall Street Reform Act. He has lectured on competition policy and media at Columbia University, Harvard Law, Duke Law, Bertelsmann Foundation, Vrije Universiteit Brussel, West Point and the National Communications Commission of Taiwan. His writing has appeared in the Washington Post, the New York Times,

Fast Company, Foreign Policy, the Guardian, Vice, The American Conservative, and the Baffler.

Joel Thayer, President of the Digital Progress Institute, previously was an associate at Phillips Lytle. Before that, he served as Policy Counsel for ACT | The App Association, where he advised on legal and policy issues related to antitrust, telecommunications, privacy, cybersecurity and intellectual property in Washington, D.C. His experience also includes working as legal clerk for FCC Chairman Ajit Pai and FTC Commissioner Maureen Ohlhausen. Additionally, Joel served as a congressional staffer for the Hon. Lee Terry and Hon. Mary Bono. Legislatures, academics, and regulators have used his submissions and articles as a source of authority to advance policies in the technology and telecommunications fields. His works have been featured in the *American University Intellectual Property Brief*, *Harvard Journal of Law and Public Policy*, *Stanford Technology Law Journal*, the *Journal of American Affairs*, the *Wall Street Journal*, *Newsweek*, *The Hill*, *The National Review*, and *The Federalist Society*.

The decision in this case will have vast implications on how the government can and ought to move forward with respect to thwarting national security threats using foreign ownership restrictions. If this Court grants Petitioners' relief, then it

would create an extraordinary cybersecurity loophole untethered from traditional notions and understandings of how foreign ownership restrictions operate. By extension, such a ruling would create a roadmap for foreign enemies to use when they seek to pilfer sensitive consumer data from our population.

Amici Curiae are a bipartisan group of policy and legal experts who have extensively researched the intersection of tech regulation and constitutionality. *Amici* join together to provide the Court with their understanding of the application of different strands of the relevant jurisprudence to the lawfulness of the potential relief sought by Petitioners. *Amici* share the view that the Protecting Americans from Foreign Adversary Controlled Applications Act ("PAFACAA" or the "Act") follows a fairly traditional path that several courts have found to pass constitutional muster. Here, *Amici* believe Petitioners have put forward weak justifications when asserting that the Act is either an unprecedented act, unconstitutional, or a rapid departure from other similarly-situated foreign ownership laws.

INTRODUCTION AND SUMMARY OF ARGUMENT

The information wars are upon us and our enemies are leveraging our own technology against us to get the upper hand. If this Court rules in favor of Petitioners, it would open the door for known corporate affiliates of the Chinese, Russian, North Korean, and Iranian governments to weaponize our Constitution to spy on our population. Here, we explain that the Protecting Americans from Foreign

Adversary Controlled Applications Act ("PAFACAA" or the "Act") follows a traditional and constitutionally sound path to thwart that threat by placing foreign ownership restrictions at the application layer. To demonstrate this, we begin with a descriptive account of foreign ownership restrictions and dispel the parochial concerns Petitioners raise with respect to the First Amendment, due process, and the Constitution's prohibition on bill of attainders.

In sum, we demonstrate that the Act's goal of keeping foreign adversaries' peering eyes out of our homes, our thoughts, and our everyday lives is imbedded in our Constitution, and that the Act's structure is consistent with the legal principles that grow out of it.

ARGUMENT

I. PAFACAA Follows a Traditional Legal Path to Thwart National Security Threats that Consistently withstand Constitutional Scrutiny

Petitioners' brief makes a series of strident claims with respect to PAFACAA, calling it "unprecedented" and a "radical departure" from the way in which the United States operates with respect to addressing national security threats. Pet Br. p. 1. Both are categorically untrue.

Social media is by far the most pervasive form of communications we have. Millions of Americans use these platforms every month. Users express their opinions and communicate with others about a wide range of social, political, and

business issues. And each platform claims to have safeguards to protect the privacy and security of U.S. user data.

But of the more than a dozen social media platforms, only one has been repeatedly caught endangering the security of the United States: TikTok. As FBI Director Christopher Wray has warned, TikTok "is a tool that is ultimately within the control of the Chinese government—and it, to me, screams out with national security concerns." Michael Martina & Patricia Zengerle, *FBI chief says TikTok 'screams' of US national security concerns*, REUTERS (Mar. 9, 2023), https://bit.ly/45jtX3z. President Biden's Director of National Intelligence Avril Haines has said that China uses apps (like TikTok) and communication networks to "develop[] frameworks for collecting foreign data and pulling it in . . . to target audiences for information campaigns or for other things." Andrea Mitchell Report, *DNI Avril Haines: Parents 'should be' concerned about kids' privacy and data on Tik-Tok*, MSNBC (Dec. 5, 2022), https://on.msnbc.com/3OWZn97.

Worse, TikTok's promises to protect the privacy and security of American data have proven hollow. Leaked audio from internal TikTok meetings shows that, at least through January 2022, engineers in China had access to U.S. data. 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), https://bit.ly/3QXXf3n. "Everything is seen in China," said one member of

TikTok's Trust and Safety team. *Id.* And eight different U.S. employees explained having to repeatedly turn to Chinese colleagues because U.S. staff "did not have permission or knowledge of how to access the data on their own." *Id.* Meanwhile, TikTok's parent ByteDance has admitted to tracking at least two U.S.-based journalists, Clare Duffy, *TikTok confirms that journalists data was accessed by employees of its parent company*, CNN (Dec. 22, 2022), https://cnn.it/3KYVYFB, and reports show that ByteDance had in fact intended to use TikTok to monitor specific American citizens. Emily Baker-White, *TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens*, FORBES (Oct. 20, 2022), https://bit.ly/44sSvWw. The U.S. Department of Justice is investigating this spying. Alexander Mallin & Luke Barr, *DOJ investigating TikTok owners for possible surveillance of US journalists: Sources*, ABC NEWS (Mar. 17, 2023), https://abcn.ws/47Pr2Bm.

These revelations are unsurprising to those who understand the intimate relationship between the Chinese government and large Chinese companies like ByteDance. To ensure alignment with Beijing's policies, ByteDance has had an internal party committee as part of its governance structure since 2017. Yaqiu Wang, *Targeting TikTok's privacy alone misses a larger issue: Chinese state control*, HUMAN RIGHTS WATCH (Jan. 24, 2020), https://bit.ly/3EgQXEA. TikTok CEO Shou Zi Chew served as ByteDance's CFO for most of 2021 and before that

was president of international operations for Xiaomi Technology, a software developer the Pentagon considers a "Communist Chinese military company." Jerry Dunleavy, *TikTok CEO's Chinese government ties in spotlight ahead of Capitol Hill testimony*, WASHINGTON EXAMINER (Mar. 23, 2023), https://bit.ly/44ovQuA.

Against this background, Congress determined that TikTok's malignancy concerned ByteDance's ownership interest and passed the Act, which places a restriction on foreign ownership on communications networks, in this case mobile and web-based apps, to combat national security threats posed by the governments of Iran, China, North Korea, and Russia owning those services.

The legal pathway the Act takes is, frankly, a well-worn one to address national security threats in the economic sector. *First,* it may surprise the Petitioners to know that the precedent for the government taking these measures to combat such a threat dates date back to our nation's founding. Alexander Hamilton cautioned that "foreign powers also will not be idle spectators. They will interpose, the confusion will increase, and a dissolution of the Union ensue." https://avalon.law.yale.edu/18th_century/debates_618.asp.

Skepticism towards foreign government influences is also embedded within our Constitution. For instance, the Constitution requires congressional candidates to be U.S. citizens for seven years. Zephyr Teachout, *Critics of the TikTok Bill Are Missing the Point*, THE ATLANTIC (Mar. 20, 2024),

https://www.theatlantic.com/ideas/archive/2024/03/tiktok-bill-foreign-influence/677806/. Moreover, our Constitution requires that our president be a natural-born citizen. *Id.* Even the treaty-ratification rule in the Constitution, which requires a two-thirds congressional vote, was included in order to reduce, as James Madison described, "the power of foreign nations to obstruct our retaliating measures on them by a corrupt influence." *Id.*

Second, the U.S. has especially applied foreign ownership restrictions in the communications sector because of its direct link to our national security. Driven by fears that foreign adversaries would use their communications companies' radio monopolies to influence policy in the U.S., Congress passed the Federal Radio Act that authorized the Federal Radio Commission (now the Federal Communications Commission ("FCC" or "Commission")) to license radio companies, and added a 20% limit on foreign stockholding to the restrictions from the 1912 Act. Ganesh Sitaramen *The Regulation of Foreign Platforms*, 74 Stan. L. Rev. 1073 (2022).

This carried through with Congress enacting the Communications Act of 1934. Specifically, Section 310 of the Communications Act prohibits a foreign government or its representative from holding any radio license. 47 U.S.C. § 310(a)-(b). Section 310 even has a broader remit than PAFACAA by applying to all foreign ownership, not just foreign adversaries.

What is more, Section 214 of the Communications Act allows the Commission to act on applications filed by carriers to provide international telecommunications service and to transfer or assign existing authorizations. 47 U.S.C. § 214. The international portion of Section 214's process ensures that the U.S. market is protected against potential anti-competitive behavior by a carrier with market power in a foreign country. 47 C.F.R § 63.21. Indeed, the FCC denied China Mobile's application to provide communications services in the United States under this provision and was upheld by this Court. *China Telecom (Americas) Corp. v. F.C.C.*, 57 F.4th 256 (D.C. Cir. 2022). This Court found that it was constitutionally permissible for the FCC to use Section 214 to deny China Telecom the ability to operate domestic and international transmission lines due to concerns about Chinese cyber threats targeting the U.S. *Id.* This Court has even upheld the FCC using its Section 214 authority to revoke a carrier's license when its indirect ownership interests from a foreign adversary poses a national security threat. *Pacific Networks Corp. & ComNet (USA), LLC v. F.C.C., et al.*, 77 F.4th 1160 (D.C. Cir. 2023).

The FCC also used Section 254 of the Communications Act to deny Huawei and ZTE monies from its Universal Service Fund on national security grounds. The Fifth Circuit upheld the FCC's decision. *Huawei Tech., Inc., et al. v. F.C.C.*, 2 F.4th 421 (5th Cir. 2021). Similarly, Congress passed the Secure and Trusted

Communications Networks Act of 2019, requiring the FCC to create a "covered" list of telecommunications equipment that pose a national security threat on the basis of the company's ownership interest. As these examples evince, the Act's approach is far from a departure and certainly not unprecedented.

FACCA's national security remit is consistent with previous legislative efforts that have been upheld by the courts, including this one. Even the specific national security threat is starkly similar to the ones present in *China Telecom*, *Pacific Networks*, and *Huawei* in that the CCP's ability to control TikTok's platform is linked to their ownership interest. However, TikTok's access to data is far more pervasive than that of Huawei or ZTE because of the app's ability to remotely access devices, engage in exfiltration data from photos, and covertly manipulate the information space. Those are the three core components that make the national security threat of foreign ownership today even more serious previous examples upheld by this court.

Third, for those companies not operating under an FCC license, the U.S. has consistently used divestiture as the primary remedy to address national security concerns with respect to foreign ownership. For instance, the Department of Treasury's Committee on Foreign Investment in the United States ("CFIUS") is a U.S. federal interagency body that is authorized to review certain foreign investment transactions in the United States that pose a threat to national security

under section 721 of the Defense Production Act of 1950, as amended, and Regulations Pertaining to Certain Investments in the United States by Foreign Persons. U.S. Dept. of the Treasury, *The Committee on Foreign Investment in the United States (CIFIUS)*, Website (last visited, Aug. 2, 2024), https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius#:~:text=The%20Committee%20on%20Foreign%20Investment%20in%20the%20United%20States%20(CFIUS),-You%20can%20now.

Transactions that may trigger CFIUS review include those that may involve certain critical technologies, critical infrastructure, or sensitive personal data. This includes online and mobile apps, which was precisely the case for the LGBTQ-dating app Grindr. In that case, CFIUS required the Chinese owners, Beijing Kunlun Tech ("Kunlun"), to divest out of Grindr to quell the noted national security threats associated with Kunlun's relationship with the CCP. *See* Sarah Bauerle Danzman & Geoffrey Gertz, *Is It a Threat to US Security that China Owns Grindr, a Gay Dating App?*, Brookings (Apr. 8, 2019), https://www.brookings.edu/articles/is-it-a-threat-to-us-security-that-china-owns-grindr-a-gay-dating-app/. Interestingly, CFIUS did not provide any insight as to the specific national security threat Grindr posed to the U.S.—although some speculate that the agency was concerned with "the Chinese government's potential

to [use Grindr to] blackmail Americans, potentially including American officials, with data from the app." Christopher Kane, *Before TikTok, the US Took Action Over National Security Concerns with Grindr*, National LGBT Media Association (Mar. 18, 2024), https://watermarkonline.com/2024/03/18/before-tiktok-the-us-took-action-over-national-security-concerns-with-grindr/.

The Act, however, would not allow for such governmental opacity by requiring far more transparency into the President's determination process than is required of CFIUS under current law. Indeed, it requires the President to put all of his further determinations to add an entity as a "covered company" for public comment and submit "a public report" to Congress at least 30 days before the determinations go into effect. Sec. 2(g)(3)(B)(ii).

Even more at odds with Petitioners' blanket assertion that the Act is novel or expansive in scope is the fact that its legal remit is actually far *narrower* than the one present in the International Emergency Economic Powers Act ("IEEPA") (*i.e.,* the statute the Trump Administration leveraged to institute its Executive Order requiring ByteDance to divest the first time around). Section 1702(a) empowers the President to "investigate, regulate, or prohibit" any foreign transaction or transfers. 50 U.S.C.A. § 1702(a).

However, unlike IEEPA, PAFACAA's threshold for the President to determine that an app qualifies as an adverse foreign controlled applications is very

high. Take, for example the Trump Administration's aforementioned executive order. While the E.O. uses the same direction or control language as the Act, it imposes zero limits on the definition of foreign adversary. Meaning it could be used to go after anyone that is tied to any country, including allies. The Act, on the other hand, requires a finding that the foreign adversary-controlled app poses a "significant threat to national security," and limits those threats to those caused by the governments of Iran, China, North Korea, and Russia. Sec. 2(g)(4).

Fourth, PAFACCA's foreign ownership requirements are standard foreign ownership considerations and legal thresholds. For instance, PAFACCA requires adverse ownership of less than 20%. This is consistent with the FCC's requirement under Section 310(b)(3) of the Communications Act. Section 310(b)(3) prohibits foreign individuals, governments, and corporations from owning more than twenty percent of the capital stock of a broadcast, common carrier, or aeronautical radio station licensee. 47 U.S.C. § 310(b)(3). What is more, if the firm's foreign ownership exceeds 10%, then the FCC refers any firm's national security concerns to a "Team Telecom" review—an interagency review process made up of national security expert agencies. *In the Matter of Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, Report and Order, 35 FCC Rcd. 10927 (2020); *see also*, E.O. 13913.

Additionally, the Act's requirement for the government to show that TikTok and ByteDance are not only owned by the foreign owner but also controlled by the adverse foreign government is consistent with a slew of other current foreign ownership requirements. For instance, the Act's use of "direction or control" is a common legal phrase, used in a variety of statutes. *See, e.g.*, 18 U.S.C. § 2339(B)(h); 15 U.S.C. § 4651(6)(B)(iii); 18 U.S.C. § 951(d); 22 U.S.C. § 611(c)(1); 18 U.S.C. § 175(b)(d)(G)(ii), (I); 15 C.F.R. § 7.2. This language has particular legal meaning and would require the government to "establish" that the adverse foreign government in fact "directed or controlled [the company's] actions." *See United States v. Chung*, 659 F.3d 815, 823 (9th Cir. 2011). This high bar means more than "simply [] acting in accordance with foreign interests or [] privately pledg[e] allegiance" to that foreign interest. *United States v. Alshahhi*, No. 21-CR-371 (BMC), 2022 WL 2239624, at *4 (E.D.N.Y. June 22, 2022). It requires actual evidence of control to make that determination.

To further combat the notion of the Act being unprecedented, consider again that the Trump E.O. that sets out a far lower threshold. For it, the statute only requires an "unacceptable risk … to the security and safety of a United States person." So too would a mere undue risk of subversion of the design of the app. While PAFACAA is limited to specific types of applications, the Trump E.O. has zero limits on covered tech. In other words, it sweeps in all tech.

PAFACCA requires the President to go through an extensive interagency process even to show that a particular app is owned by a statutorily defined set of governments and is controlled in the same way China owns TikTok.

Lastly, the Act simply fills in the necessary gaps in our current federal law. The FCC has limited jurisdiction over communications systems. Indeed, the FCC's Section 214 authority only applies to "telecommunications services" that, at least for now, is limited to Internet service providers, devices, and telecommunications, not mobile or web-based applications. *See generally*, *In the Matter of Safeguarding and Securing an Open Internet, et al.*, WC Docket No. 23-320, Declaratory Ruling, et al, F.C.C. 24-52 (2024), https://docs.fcc.gov/public/attachments/FCC-24-52A1.pdf. The Act effectively covers the FCC's flank to ensure that our foreign adversaries cannot escape foreign ownership requirements by using apps outside of the FCC's jurisdiction.

CIFIUS, too, is an unreliable authority to combat the national security issues at play because its authority hinges on particular transactions occurring. 31 C.F.R. § 800.213. To start, it is unclear how the agency determines what qualifies as a "covered transaction" and gives CFIUS with fairly broad authority to approve or challenge a transaction without qualifying its decisions one way or the other. In December 2022, CFIUS determined that it did not have jurisdiction to review the proposed acquisition of North Dakota land by a Chinese company, Fufeng Group, with

the intent to build a $700 million corn milling plant without providing a scintilla of information as to why. Pat Sweeny, *Fufeng 'Looks Forward' to Building GF Plant After CFIUS Says It Has 'No Jurisdiction'*, Knox Radio News (Dec. 13, 2022), https://knoxradio.com/2022/12/13/fufeng-looks-forward-to-building-gf-plant-after-cfius-says-it-has-no-jurisdiction/. Even if CFIUS determined that a transaction qualifies, it has no authority to enforce compliance with its decisions, as they are mere voluntary restrictions. The Act takes care of both of these issues because the Act defines the specific transactions with which the government is concerned; Sec. 2(g)(3)(B)(i) (defining a "foreign adversary controlled application"), and provides the government the tools to enforce compliance. Sec. 2(d) (providing the Department of Justice the authority to enforce compliance with the President's or Congress's determination).

* * *

In sum, Petitioners' claims that the Act's measures are either novel or radical are flatly contradicted by multiple judicial and legislative precedents.

II. The Narrow Focus on Foreign Ownership of PAFACAA is Attuned to Constitutional Considerations

Petitioners argue that the Act runs afoul the constitution in several ways. They assert that PAFACAA is a speech regulation that implicates the First Amendment, and that the Act explicitly listing ByteDance and TikTok in its definition of a foreign adversary controlled application violates their due

process rights and makes the Act an unlawful bill of attainder. We discuss, in turn, how the Act amounts to nothing of the sort and is consistent with traditional understandings of those constitutional doctrines.

a. How Foreign Ownership Restrictions Relate to the First Amendment

To start, we exclude foreign citizens from myriad First Amendment activities. As then-District Court Judge (now Justice) Kavanaugh described, the Supreme Court "has drawn a fairly clear line: The government may exclude foreign citizens from activities 'intimately related to the process of democratic self-government.'" *Bluman v. FEC*, 800 F.Supp.2d (D.D.C. 2011) (citing *Bernal v. Fainter,* 467 U.S. 216, 220 (1984); *see also Gregory v. Ashcroft,* 501 U.S. 452, 462 (1991); *Cabell v. Chavez-Salido,* 454 U.S. 432, 439–40 (1982)). The Supreme Court affirmed that decision. *Bluman v. FEC*, 565 U.S. 1104 (2012) (mem.).

Justice Kavanaugh is correct, as the U.S. has barred foreign citizens from becoming probation officers, *Cabell,* 454 U.S. at 439; teaching in public schools, *Ambach v. Norwick*, 441 U.S. 68, 75 (1979); and hiring them as police officers. *Foley v. Connelie*, 435 U.S. 291, 297 (1978). Justice Kavanaugh further explained in *Bluman* that "[i]t is fundamental to the definition of our national political community that foreign citizens do not have a constitutional right to participate in, and thus may be excluded from, activities of democratic self-government." *Bluman*, 800 F. Supp.2d at 289.

In *NetChoice v. Moody*, Justice Amy Coney Barrett indicated that granting social media platforms First Amendment protections for non-expressive conduct would be an unprecedented and damaging expansion of First Amendment jurisprudence. *NetChoice v. Moody*, 600 U.S. __ (2024) (Barrett, J., concurring) (citing *Citizens United v. Federal Election Comm'n*, 558 U. S. 310, 365 (2010); *cf. Burwell v. Hobby Lobby Stores, Inc.*, 573 U. S. 682, 706–707 (2014)). Justice Barrett goes on to say "…foreign persons and corporations located abroad" are not afforded the same protections under our Constitution as individuals or even domestic corporations. *Id*. In *Agency for Int'l Development v. Alliance for Open Society Int'l, Inc.*, the Court affirmatively stated that such a principle is "long settled law." 591 U.S. 430, 431 (2020).

However, imposing foreign ownership restrictions on communications platforms is several steps removed from such free speech concerns, because the regulations are predominately concerned with a firm's conduct rather than the content it may transmit. This is made evident by the U.S. notoriously imposing them on a wide array of foreign communications companies without raising a modicum of First Amendment scrutiny. As mentioned above, Congress passed the Secure and Trusted Communications Network Act of 2019, which directed the FCC to remove equipment associated with national security threats from American networks. Pub. Law No. 116-124. Accordingly, the Commission relied on the

views of national security experts and banned Huawei from selling any more telecommunications equipment to rural customers that rely on federal subsidies. In a similar vein, the Commission has revoked the ability of Chinese-affiliated carriers China Telecom, ComNet, and Pacific Networks from interconnecting with American telecommunications networks and operating in the United States.

The courts have blessed these prohibitions. The Fifth Circuit turned aside Huawei's federal-law and constitutional challenges. *See Huawei Technologies USA v. FCC*, 2 F.4th 421 (5th Cir. 2021). This Court upheld the revocations of China Telecom, ComNet, and Pacific Networks without a scintilla of concern towards a First Amendment violation. *See China Telecom (Americas) Corp. v. F.C.C.*, 57 F.4th 256 (D.C. Cir. 2022); *Pacific Networks Corp., et al. v. F.C.C.*, 77 F.4th 1160 (D.C. Cir. 2023).

The likely reason such restrictions do not raise concerns under the First Amendment is due to them being a conduct regulation, not a content regulation. Courts have consistently distinguished between conduct and speech in applying the First Amendment. In *Arcara v. Cloud Books, Inc.*, for example, the New York state government shut down an adult bookstore for health violations because its owner used his store to facilitate prostitution. 478 U.S. 697 (1986). Even though we think of a bookstore as a quintessential venue for First Amendment activity, the Supreme Court ruled that the First Amendment did not prevent the government from shutting

down the bookstore because the government was acting based on the owner's decision to engage in prohibited, non-speech conduct. *Id.* at 707.

As Justice Burger explained:

> The legislation providing the closure sanction was directed at unlawful conduct having nothing to do with books or other expressive activity. Bookselling 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.*

Like the health regulation against the bookstore, the Act is indifferent to the content either TikTok or ByteDance host or promote. The Act's general applicability further demonstrates this by not limiting its application to social media companies. Indeed, the Act also captures a wide-array of apps, such as food-delivery apps, online retailers, ride-sharing apps, etc. The text of the Act takes no issue with the content TikTok hosts or predicates its foreign ownership requirements on content-based considerations.

The First Amendment poses no bar to the Act or its enforcement, and finding otherwise would not only overturn decades of precedent, but would handcuff the ability of the United States to reign in large technology platforms that spy on the American people—hardly a result the framers of our Constitution would have envisioned. Hence, it is granting Petitioners' sought after relief that would be a "radical departure" from the way in which the United States operates with respect to foreign citizenship.

b. The fact that both ByteDance and TikTok have been the subject of multiple agency investigations and congressional hearings justifies the Act's specifying them in the definition of foreign adversarial controlled applications

Petitioners make vague references to the Act's supposed failure to provide them due process under the law. Pet. Br. p. 45. They claim that the Act "singling out" TikTok within its definition of an "foreign adversarial controlled application" is arbitrary and unfair. *Id.* at p. 47. Petitioners argue that the Act would deny them the ability to challenge or engage in an interagency procedure before the government makes that determination, where other prospective companies with similar ownership structures to Petitioners' could. *Id.* at ps. 44-46. The Petitioners appeal to "the equal protection component of the Due Process Clause" to make their case. *Id.* at 45.

Generally, the Supreme Court finds that "legislative Acts adjusting the burdens and benefits of economic life come to the Court with a presumption of constitutionality…." *Pension Benefit Guar. Corp. v. R.A. Gray & Co.*, 467 U.S. 717, 729 (1984). The Court has further said that "the burden is on the one complaining of a due process violation to establish that the legislature has acted in an arbitrary and irrational way." *Id.* Similar to the impacts the 2019 National Defense Authorization Act ("2019 NDAA") had on Huawei by denying its ability to contract with the U.S. government; *Huawei Tech. U.S.A., Inc., et al. v. U.S.*, 440 F.Supp.3d 607 (E.D. Tex. 2020), the Act is strictly limited to economic burdens on

TikTok and ByteDance—i.e., the denial of providing services contingent on a qualified divestiture. The question is whether listing TikTok and ByteDance is rationally related to a legitimate government interest.

The facts show that it clearly is. The Report that the CCP Select Committee concurrently submitted with the introduction of the Act demonstrates this. H. Res. 1051. The Report shows that singling out Petitioners is warranted because it is based on at least 13 investigative congressional hearings in which TikTok representatives were participants. Moreover, the Report shows that the Act's penalties and remedies in seeking divestiture are built off several reviews from CFIUS (spanning over multiple years) that TikTok also participated in. Thus, Petitioners have ample knowledge on what assets it would need to divest from to comply with the law.

Congress has also provided a rationale as to why a divestiture for ByteDance and TikTok especially is the only rational path to achieve the Act's national security goals. The Report notes the significant national security threat data leaks and privacy violations from companies can pose when controlled by a foreign adversary. It notes that:

> The Department of Homeland Security has warned that the PRC's data collection activities in particular have resulted in "numerous risks to U.S. businesses and customers, including: the theft of trade secrets, of intellectual property, and of other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service;

> security and privacy risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses". These risks are imminent and other, unforeseen risks may also exist. *See* H. Res. 1051.

TikTok's flagrant disregard of our existing privacy laws does not help its case. Its track record includes:

- In 2019 TikTok entered into a consent decree with the Federal Trade Commission for violating the Children's Online Privacy Protection Act, paying $5.7 million—a record fine. Federal Trade Commission, *Video Social Networking App Musical.ly [now TikTok] Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* (Feb. 27, 2019), https://shorturl.at/huILP.
- Not a year later, the Federal Trade Commission received a complaint that TikTok was already violating that consent decree. Campaign for a Commercial-Free Childhood et al., *Complaint and Request for Investigation of TikTok for Violations of the Children's Online Privacy Protection Act and Implementing Rule* (May 14, 2020), https://shorturl.at/bnzUZ.
- In 2022, TikTok settled a class-action lawsuit for $92 million for violating Illinois privacy law. *In re TikTok, Inc. Consumer Privacy Litigation*, MDL No. 2948, Memorandum Opinion and Order (July 28, 2022), https://shorturl.at/jlmwY.

- In early 2023, fifteen separate lawsuits alleged that TikTok illegally tracked its users in violation of the Federal Wiretap Act. Cyrus Farivar, *TikTok's In-App Browser Monitoring Violates Wiretap Law, Slew of Lawsuits Claim*, FORBES (Mar. 3, 2023), https://shorturl.at/epqtJ.
- That same year, a group of 46 state attorneys general complained that TikTok had failed to preserve subpoenaed evidence and refused to produce that evidence in a readable format in a lawsuit regarding TikTok's compliance with state privacy and consumer protection laws. *In re Investigation of TikTok, Inc.*, Brief of Amici Curiae The Colorado Department of Law and 45 Other States in Common Interest (Mar. 6, 2023), https://shorturl.at/exDP5.

Given that TikTok's 'data-security' measures leak like a sieve, and ByteDance may almost certainly be its repository to collect the estranged data, a law untethering them is the most effective and least restrictive way to quell the unique national security threat the relationship poses for the United States.

It is also important to note that a law listing specific companies is not, on its own, a due process violation. Precedent concerning Huawei is instructive here. Indeed, the Eastern District of Texas found that the 2019 NDAA did not violate Huawei's due process rights by explicitly listing it in the statute, even though doing

so would have the effect of prohibiting the government from contracting with the company to procure its telecom equipment. *Huawei Tech. U.S.A., Inc.*, *et al. v. U.S.*, 440 F.Supp.3d 607 (E.D. Tex. 2020). The Eastern District of Texas found for the government on the grounds that "legislation is not presumptively unconstitutional simply because it applies with specificity." *Id.* at 651 (citing *Bank Markazi v. Peterson*, 578 U.S. 212 (2016)). The court even doubled down by saying that "laws of general applicability are "by no means [the legislature's] only legitimate mode of action."" (citing *Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 239 n.9 (1995)).

The due process claim, as it was when proffered by Huawei, is simply unsupported.

c. *Courts have even upheld naming specific companies as threats in legislation*

The Bill of Attainder Clause, Article I, Section 9, Clause 3 of the Constitution, prohibits a legislative act that inflicts punishment without a judicial trial. But "it does not do so by limiting Congress to the choice of legislating for the universe, or legislating only benefits, or not legislating at all." *Nixon v. Adm'r of General Services*, 433 U.S. 425, 428 (1977). Rather, Congress may legislate even when only a single individual or company is the subject of the legislation.

Like general due process, the Constitution requires more than specificity, it also requires a *retroactive punishment*. In *Selective Serv. Sys. v. Minn. Pub.*

Interest Research Grp., the Supreme Court laid out a three-part test to determine whether legislative action constitutes a punishment rather than a mere burden. 468 U.S. 841 (1984). The historical test asks "whether the challenged statute falls within the historical meaning of legislative punishment." *Id.* at 852. The functional test asks whether the statute, "viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes." *Id.* And the motivational tests asks whether the legislative record "evinces a congressional intent to punish." *Id.* A successful claim requires that all three tests be met. *Id.*

Huawei is again the most direct precedent. In *Huawei*, the District Court held that Congress's actions against Huawei were lawful because it was not denying Huawei a trial for past offenses even though the 2019 NDAA specifically listed Huawei in the statute. 440 F.Supp.3d at 637. Instead, the court found that the NDAA applied to transactions that have not yet occurred and thus fell outside the scope of the type of punishment necessary to be considered a bill of attainder. *Id.*

This is where Petitioners' argument falls apart. The Act pertains to future conduct, not conduct that has already occurred. Congress did not impose or demand any recompense for TikTok's past wrongs—it only prohibited TikTok from continuing to operate its app in the United States starting either 270 days or 1 year

(depending on the President's allotted discretion) after the Act's enactment if it continued to pose a threat by maintaining its relationship with ByteDance.

Compare this to the facts in *U.S. v. Lovett* where Congress prohibited paying the salaries for a few dozen federal employees via the Urgent Deficiency Appropriation Act of 1943 because Congress thought their affiliation with the Communist Party violated federal law. 328 U.S. 303, 306 (1946). The Supreme Court held that by doing so Congress was playing the role of a court and, hence, punished the past conduct of employees without a trial. *Id.* at 315-16.

Again, the Bill of Attainder Clause poses no barrier to the implementation of the Act. Instead, the Constitution gives Congress broad flexibility to craft legislation to thwart the attempts of foreign governments to use technology to spy on Americans.

* * *

In sum, Petitioners have put forward weak justifications when asserting that the Act is either an unprecedented act or a rapid departure from other similarly-situated foreign ownership laws, or that it violates the constitution.

CONCLUSION

For all of the foregoing reasons, the Court should deny Petitioners' relief.

Dated: August 2, 2024

Respectfully submitted,

/s/ Joel L. Thayer
Joel L. Thayer
Thayer, PLLC
1255 Union Street, 7th Floor
Washington, D.C. 20002
JThayer@thayer.tech
p. (760) 668-0934

Attorney for Amici Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify, on August 2, 2024, that:

1. This document complies with the word limit under Federal Rule of Appellate Procedure 32(a)(7) because, excluding the parts of the document exempted by Federal Rule of Appellate Procedure 32(f), this document contains 6,207 words.

2. This document complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this document was prepared in a proportionally spaced typeface using Microsoft Word for Office 365 MSO in a 14-point Times New Roman font.

Respectfully submitted,

/s/ Joel L. Thayer
Joel L. Thayer
Thayer, PLLC
1255 Union Street, 7th Floor
Washington, D.C. 20002
JThayer@thayer.tech
p. (760) 668-0934

Attorney for Amici Curiae