

**IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

---

TIKTOK INC.,

and

BYTEDANCE LTD.,

*Petitioners,*

v.

No. 24-1113

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

*Respondent.*

---

**PETITION FOR REVIEW OF  
CONSTITUTIONALITY OF THE  
PROTECTING AMERICANS FROM FOREIGN  
ADVERSARY CONTROLLED APPLICATIONS ACT**

1. Congress has taken the unprecedented step of expressly singling out and banning TikTok: a vibrant online forum for protected speech and expression used by 170 million Americans to create, share, and view videos over the Internet. For the first time in history, Congress has enacted a law that subjects a single, named speech platform to a permanent, nationwide ban, and bars every American from participating in a unique online community with more than 1 billion people worldwide.

2. That law — the Protecting Americans From Foreign Adversary Controlled Applications Act (the “Act”) — is unconstitutional. Banning TikTok is so obviously unconstitutional, in fact, that even the Act’s sponsors recognized that reality, and therefore have tried mightily to depict the law not as a ban at all, but merely a regulation of TikTok’s ownership. According to its sponsors, the Act responds to TikTok’s ultimate ownership by ByteDance Ltd., a company with Chinese subsidiaries whose employees support various ByteDance businesses, including TikTok. They claim that the Act is not a ban because it offers ByteDance a choice: divest TikTok’s U.S. business or be shut down.<sup>1</sup>

---

<sup>1</sup> References to “TikTok Inc.” are to the specific U.S. corporate entity that is a Petitioner in this lawsuit and publishes the TikTok platform in the

3. But in reality, there is no choice. The “qualified divestiture” demanded by the Act to allow TikTok to continue operating in the United States is simply not possible: not commercially, not technologically, not legally. And certainly not on the 270-day timeline required by the Act. Petitioners have repeatedly explained this to the U.S. government, and sponsors of the Act were aware that divestment is not possible. There is no question: the Act will force a shutdown of TikTok by January 19, 2025, silencing the 170 million Americans who use the platform to communicate in ways that cannot be replicated elsewhere.

4. Of course, even if a “qualified divestiture” were feasible, the Act would still be an extraordinary and unconstitutional assertion of power. If upheld, it would allow the government to decide that a company may no longer own and publish the innovative and unique speech

---

United States. References to “TikTok” are to the online platform, which includes both the TikTok mobile application and web browser experience. References to “ByteDance Ltd.” are to the specific Cayman Islands-incorporated holding company that is identified in the Act and is a Petitioner in this lawsuit. References to “ByteDance” are to the ByteDance group, inclusive of ByteDance Ltd. and relevant operating subsidiaries. TikTok Inc. and ByteDance. Ltd. are together referred to as “Petitioners.”

platform it created. If Congress can do this, it can circumvent the First Amendment by invoking national security and ordering the publisher of any individual newspaper or website to sell to avoid being shut down. And for TikTok, any such divestiture would disconnect Americans from the rest of the global community on a platform devoted to shared content — an outcome fundamentally at odds with the Constitution’s commitment to both free speech and individual liberty.

5. There are good reasons why Congress has never before enacted a law like this. Consistent with the First Amendment’s guarantee of freedom of expression, the United States has long championed a free and open Internet — and the Supreme Court has repeatedly recognized that speech “conveyed over the Internet” fully qualifies for “the First Amendment’s protections.” *303 Creative LLC v. Elenis*, 600 U.S. 570, 587 (2023). And consistent with the fundamental principles of fairness and equal treatment rooted in the Bill of Attainder Clause and the Fifth Amendment, Congress has never before crafted a two-tiered speech regime with one set of rules for one named platform, and another set of rules for everyone else.

6. In dramatic contrast with past enactments that sought to regulate constitutionally protected activity, Congress enacted these extreme measures without a single legislative finding. The Act does not articulate any threat posed by TikTok nor explain why TikTok should be excluded from evaluation under the standards Congress concurrently imposed on every other platform. Even the statements by individual Members of Congress and a congressional committee report merely indicate concern about the *hypothetical* possibility that TikTok could be misused in the future, without citing specific evidence — even though the platform has operated prominently in the United States since it was first launched in 2017. Those speculative concerns fall far short of what is required when First Amendment rights are at stake.

7. Nor is there any indication that Congress considered any number of less restrictive alternatives, such as those that Petitioners developed with the Executive Branch after government agencies began evaluating the security of U.S. user data and the risk of foreign government influence over the platform's content as far back as 2019. While such concerns were never substantiated, Petitioners nevertheless

worked with the government for four years on a voluntary basis to develop a framework to address the government's concerns.

8. As part of this engagement, Petitioners have voluntarily invested more than \$2 billion to build a system of technological and governance protections — sometimes referred to as “Project Texas” — to help safeguard U.S. user data and the integrity of the U.S. TikTok platform against foreign government influence. Petitioners have also made extraordinary, additional commitments in a 90-page draft National Security Agreement developed through negotiations with the Committee on Foreign Investment in the United States (“CFIUS”), including agreeing to a “shut-down option” that would give the government the authority to suspend TikTok in the United States if Petitioners violate certain obligations under the agreement.

9. Congress tossed this tailored agreement aside, in favor of the politically expedient and punitive approach of targeting for disfavor one publisher and speaker (TikTok Inc.), one speech forum (TikTok), and that forum's ultimate owner (ByteDance Ltd.). Through the Act's two-tiered structure, Congress consciously eschewed responsible industry-wide regulation and betrayed its punitive and discriminatory purpose.

Congress provided every other company — however serious a threat to national security it might pose — paths to avoiding a ban, excluding only TikTok Inc. and ByteDance Ltd. Indeed, for any other company’s application to be banned, Congress mandated notice and a “public report” describing “the specific national security” concern, accompanied by supporting classified evidence. For Petitioners only, however, there is no statement of reasons and no supporting evidence, with any discussion of the justifications for a ban occurring only behind closed doors.

10. Congress must abide by the dictates of the Constitution even when it claims to be protecting against national security risks: “against [those] dangers . . . as against others, the principle of the right to free speech is always the same.” *Abrams v. United States*, 250 U.S. 616, 628 (1919) (Holmes, J., dissenting). Congress failed to do so here, and the Act should be enjoined.

### **Jurisdictional Statement**

11. Pursuant to Sections 3(a) and 3(b) of the Act, H.R. 815, div. H, 118th Cong., Pub. L. No. 118-50 (April 24, 2024), this Court has original

and exclusive jurisdiction over this challenge to the constitutionality of the Act.<sup>2</sup>

### **Background and Nature of Proceedings**

#### **A. TikTok Is a Speech Platform Used by 170 Million Americans.**

12. TikTok is an online video entertainment platform designed to provide a creative and entertaining forum for users to express themselves and make connections with others over the Internet. More than 170 million Americans use TikTok every month, to learn about and share information on a range of topics — from entertainment, to religion, to politics. Content creators use the TikTok platform to express their opinions, discuss their political views, support their preferred political candidates, and speak out on today’s many pressing issues, all to a global audience of more than 1 billion users. Many creators also use the

---

<sup>2</sup> A copy of the Act is attached to this Petition as Exhibit A. Because this Petition does not involve a challenge to any agency action, it is not governed by Federal Rule of Appellate Procedure 15(a). Petitioners intend to file a separate motion regarding the procedures governing this original proceeding. Petitioners summarize the pertinent facts and claims below to facilitate this Court’s review consistent with the practice of a case-initiating pleading in a court of original jurisdiction, but reserve their rights to present additional facts and arguments in due course.



platform to post product reviews, business reviews, and travel information and reviews.

13. In the United States, the TikTok platform is provided by TikTok Inc., a California-incorporated company that has its principal place of business in Culver City, California and offices in New York, San Jose, Chicago, and Miami, among other locations. TikTok Inc. has thousands of employees in the United States. Like many platforms owned by companies that operate globally, the global TikTok platform is supported not only by those employees, but also by employees of other ByteDance subsidiaries around the globe, including in Singapore, the United Kingdom, Brazil, Germany, South Africa, Australia, and China. Many of the global TikTok platform's functions are spread across different corporate entities and countries, and the global TikTok business is led by a leadership team based in Singapore and the United States. Like other U.S. companies, TikTok Inc. is governed by U.S. law.

14. TikTok Inc.'s ultimate parent company is ByteDance Ltd., a Cayman Islands-incorporated equity holding company. ByteDance was founded in 2012 by Chinese entrepreneurs. Over time, the company sought funding to fuel growth, as is common in the technology sector,

which resulted in the issuance of additional equity and the dilution of existing shares. Today, approximately 58 percent of ByteDance Ltd. is owned by global institutional investors (such as BlackRock, General Atlantic, and Susquehanna International Group), 21 percent is owned by the company's founder (a Chinese national who lives in Singapore), and 21 percent is owned by employees — including approximately 7,000 Americans.

15. ByteDance launched TikTok in May 2017 in over 150 countries, including the United States.<sup>3</sup> Since its launch, TikTok has become one of the world's most popular applications, with over 1 billion users worldwide. As of January 2024, more than 170 million Americans use TikTok on a monthly basis.

16. Users primarily view content on TikTok through its “For You” page, which presents a collection of videos curated by TikTok's proprietary recommendation engine. The recommendation engine customizes each user's content feed based on how the user interacts with

---

<sup>3</sup> TikTok was later relaunched in August 2018 following a transaction involving the company Musical.ly. *See generally* Petition for Review, *TikTok Inc. v. CFIUS*, No. 20-1444 (D.C. Cir. Nov. 10, 2020).

the content that the user watches. TikTok's popularity is based in large part on the effectiveness of the recommendation engine. The source code for TikTok's recommendation engine was originally developed by ByteDance engineers based in China, and the engine is customized for operations in TikTok's various global markets, including in the United States. TikTok is not offered in mainland China.

17. Aside from TikTok, ByteDance has developed and operates more than a dozen other online platforms and software applications for use in U.S. and international markets, including for content-sharing, video and music editing, e-commerce, gaming, and enterprise productivity.

**B. The Government Previously Made Unlawful Attempts to Ban TikTok.**

18. Petitioners' efforts to address the U.S. government's asserted concerns regarding the TikTok platform date back to 2019. At that time, Petitioners began engaging with CFIUS, which had initiated a review of ByteDance Ltd.'s 2017 acquisition of Musical.ly, another Internet-based video-sharing platform.

19. Petitioners were in the early stages of engaging with CFIUS on a voluntary basis to address the government's concerns, when on August 6, 2020, President Trump abruptly issued an executive order purporting to ban TikTok under the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701–08. *See* 85 Fed. Reg. 48,637 (the "Ban Order"). Two separate district courts preliminarily enjoined the Ban Order, concluding (among other things) that it exceeded the President's IEEPA authority. *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 83 (D.D.C. 2020); *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 112 (D.D.C. 2020); *Marland v. Trump*, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020).

20. Specifically, as these courts correctly recognized, the President's IEEPA authority "to deal with any unusual and extraordinary threat" to the nation "does not include the authority to regulate or prohibit, directly or indirectly . . . [any] personal communication" or the importation or exportation "of any information or informational materials." 50 U.S.C. § 1702(b)(1), (3). These restrictions on the President's IEEPA authority — which Congress expanded through multiple amendments to the statute — were designed "to prevent the statute from running afoul of the First Amendment." *United States v.*

*Amirnazmi*, 645 F.3d 564, 585 (3d Cir. 2011) (quotation marks omitted); *see also Kalantari v. NITV, Inc.*, 352 F.3d 1202, 1205 (9th Cir. 2003) (IEEPA’s limitations necessary “to prevent the executive branch from restricting the international flow of materials protected by the First Amendment”); *Marland*, 498 F. Supp. 3d at 629 (same).

21. Looking to the foundational First Amendment principles codified in IEEPA’s text and legislative history, these courts concluded that President Trump’s efforts to ban TikTok violated the statute and raised “serious” constitutional questions (which were unnecessary to decide under the doctrine of constitutional avoidance). *TikTok Inc.*, 507 F. Supp. 3d at 112 n.6; *TikTok Inc.*, 490 F. Supp. 3d at 83 n.3. The courts granted the government’s motions to voluntarily dismiss its appeals after President Biden withdrew the Ban Order. *See TikTok Inc. v. Biden*, No. 20-5302, 2021 WL 3713550 (D.C. Cir. July 20, 2021); *TikTok Inc. v. Biden*, No. 20-5381, 2021 WL 3082803 (D.C. Cir. July 14, 2021); *Marland v. Trump*, No. 20-3322, 2021 WL 5346749 (3d Cir. July 14, 2021).

22. Separately, acting on a CFIUS referral, President Trump on August 14, 2020 issued an order under Section 721 of the Defense Production Act, 50 U.S.C. § 4565, purporting to direct ByteDance to

divest from TikTok's U.S. business and U.S. user data. 85 Fed. Reg. 51,297 (the "Divestment Order"). On November 10, 2020, Petitioners petitioned this Court for review of the Divestment Order and underlying CFIUS actions, arguing, among other things, that the government lacked jurisdiction under the statute. *See* Petition for Review, *TikTok Inc. v. CFIUS*, No. 20-1444 (D.C. Cir. Nov. 10, 2020). That petition was held in abeyance in February 2021 on the parties' joint motion to allow the parties to negotiate a resolution. The government has filed status reports every 60 days since then, most recently on April 22, 2024. Those status reports have consistently reported that "[t]he parties continue to be involved in ongoing negotiations" and "[a]beyance continues to be appropriate." *See, e.g.*, Status Report, *TikTok Inc. v. CFIUS*, No. 20-1444 (D.C. Cir. Apr. 22, 2024).

23. Between January 2021 and August 2022, Petitioners and CFIUS engaged in an intensive, fact-based process to develop a National Security Agreement that would resolve the U.S. government's concerns about whether Chinese authorities might be able to access U.S. user data or manipulate content on TikTok, as well as resolve the pending CFIUS dispute. During that time, Petitioners and government officials

communicated regularly, often several times a week — including several in-person meetings — about the government’s concerns and potential solutions. The result was an approximately 90-page draft National Security Agreement with detailed annexes embodying a comprehensive solution addressing the government’s national security concerns. Notably, the draft National Security Agreement provided that all protected U.S. user data (as defined in the agreement) would be stored in the cloud environment of a U.S.-government-approved partner, Oracle Corporation, which would also review and vet the TikTok source code.

24. From Petitioners’ perspective, all indications were that they were nearing a final agreement. After August 2022, however, CFIUS without explanation stopped engaging with Petitioners in meaningful discussions about the National Security Agreement. Petitioners repeatedly asked why discussions had ended and how they might be restarted, but they did not receive a substantive response. In March 2023, without providing any justification for why the draft National Security Agreement was inadequate, CFIUS insisted that ByteDance would be required to divest the U.S. TikTok business.

25. Since March 2023, Petitioners have explained to CFIUS, in multiple written communications and in-person meetings, that a divestiture of the U.S. TikTok business from the rest of the integrated global TikTok platform and business of the sort now required by the Act is not feasible. CFIUS has never articulated any basis for disagreeing with that assessment, offering instead only a conclusory assertion that the reason ByteDance was not divesting was because it was simply unwilling to do so. The Act nonetheless incorporates precisely such an infeasible divestiture standard.

**C. A Divestiture that Severs TikTok's U.S. Operations From the Rest of the Globally Integrated TikTok Business Is Not Commercially, Technologically, or Legally Feasible.**

26. The Act purports to allow Petitioners to avoid a ban by executing a “qualified divestiture.” Sec. 2(c). But that alternative is illusory because, as Petitioners have repeatedly explained to CFIUS, the divestiture of the TikTok U.S. business and its severance from the globally integrated platform of which it is an integral part is not commercially, technologically, or legally feasible.



27. *First*, a standalone U.S. TikTok platform would not be commercially viable. TikTok and its competitors are globally integrated platforms where content created in one country is available to users in other countries. Indeed, a substantial part of TikTok’s appeal is the richness of the international content available on the platform — from global sporting events like the Olympics to international K-pop stars from South Korea, as well as videos created by U.S. creators and enjoyed by audiences worldwide. A divestment of the U.S. TikTok platform, without any operational relationship with the remainder of the global platform, would preclude the interoperability necessary to make international content seamlessly available in the U.S. market and vice versa. As a result, the U.S. TikTok platform would become an “island” where Americans would have an experience detached from the rest of the global platform and its over 1 billion users. Such a limited pool of content, in turn, would dramatically undermine the value and viability of the U.S. TikTok business.<sup>4</sup>

---

<sup>4</sup> The contemplated qualified divestiture would also undercut the important role currently played by American voices in the global conversation ongoing on TikTok.

28. *Second*, precipitously moving all TikTok source code development from ByteDance to a new TikTok owner would be impossible as a technological matter. The platform consists of millions of lines of software code that have been painstakingly developed by thousands of engineers over multiple years. Although much of this code is basic infrastructure for running the global TikTok platform and has nothing at all to do with TikTok’s recommendation algorithm, the statute requires that *all* of this code be wrested from Petitioners, so that there is no “operational relationship” between ByteDance and the new U.S. platform. Specifically, to comply with the law’s divestiture requirement, that code base would have to be moved to a large, alternative team of engineers — a team that does not exist and would have no understanding of the complex code necessary to run the platform. It would take years for an entirely new set of engineers to gain sufficient familiarity with the source code to perform the ongoing, necessary maintenance and development activities for the platform. Moreover, to keep the platform functioning, these engineers would need access to ByteDance software tools, which the Act prohibits. Such a fundamental rearchitecting is not

remotely feasible on anything approaching the 270-day timeframe contemplated by the Act.

29. *Third*, the Chinese government has made clear that it would not permit a divestment of the recommendation engine that is a key to the success of TikTok in the United States. Like the United States,<sup>5</sup> China regulates the export of certain technologies originating there. China's export control rules cover "information processing technologies" such as "personal interactive data algorithms."<sup>6</sup> China's official news agency has reported that under these rules, any sale of recommendation algorithms developed by engineers employed by ByteDance subsidiaries in China, including for TikTok, would require a government license.<sup>7</sup>

---

<sup>5</sup> For example, the U.S. Department of Commerce has issued restrictions on the export to China of advanced chips that can be used to train artificial intelligence models. *E.g.*, Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections, 88 Fed. Reg. 73458 (Oct. 25, 2023) (to be codified at 15 C.F.R. § 732.2 *et seq.*).

<sup>6</sup> See Karen M. Sutter, Cong. Rsch. Serv., IN11524, China Issues New Export Control Law and Related Policies 2 (2020).

<sup>7</sup> Paul Mozur, Raymond Zhong & David McCabe, *TikTok Deal Is Complicated by New Rules From China Over Tech Exports*, N.Y. Times (Aug. 29, 2020), <https://perma.cc/L6RB-CTT9>.

China also enacted an additional export control law that “gives the Chinese government new policy tools and justifications to deny and impose terms on foreign commercial transactions.”<sup>8</sup> China adopted these enhanced export control restrictions between August and October 2020, shortly after President Trump’s August 6, 2020 and August 14, 2020 executive orders targeting TikTok. By doing so, the Chinese government clearly signaled that it would assert its export control powers with respect to any attempt to sever TikTok’s operations from ByteDance, and that any severance would leave TikTok without access to the recommendation engine that has created a unique style and community that cannot be replicated on any other platform today.

**D. The Act Bans TikTok and Other ByteDance Applications.**

30. On April 24, 2024, the President signed the Protecting Americans from Foreign Adversary Controlled Applications Act.

31. The Act prohibits, on pain of draconian penalties, “online mobile application store[s]” and “internet hosting services” from servicing “foreign adversary controlled application[s]” within the United States.

---

<sup>8</sup> Sutter, *supra* n.6.

See Sec. 2(a), 2(d)(1)(A). This includes the “distribution, maintenance, or updating” of a covered application through an online marketplace. Sec. 2(a)(1).

32. Section 2(g)(3) creates two classes of “foreign adversary controlled applications” covered by the Act.

33. The first class singles out only one corporate group: “ByteDance[] Ltd.,” “TikTok,” their “subsidiar[ies] or successor[s]” that are “controlled by a foreign adversary,” or any entity “owned or controlled” by the aforementioned.<sup>9</sup> The Act deems *any* application operated by these entities a “foreign adversary controlled application,” without any finding about why any particular application — much less every application operated by these entities — should be so designated. See Sec. 2(g)(3)(A).

---

<sup>9</sup> “TikTok” is a platform, not a legal entity. Petitioners assume that Congress intended this provision to be a reference to TikTok Inc., and further reserve their rights to amend this Petition to include additional TikTok entities to the extent the government takes the position that other entities are covered by this reference. In any event, TikTok Inc. is covered as an entity “owned or controlled” by ByteDance Ltd.

34. The second class creates a discretionary process by which the President can designate other companies whose applications will also effectively be banned. Under these provisions, the President may designate an application as a “foreign adversary controlled application” if several qualifications are met:

- a. *Covered Company*. The website or application is operated directly or indirectly by a “covered company” — *i.e.*, a company that operates a website or application that permits users to share content and has at least 1 million monthly active users. *See* Sec. 2(g)(2)(A).
- b. *Controlled by a Foreign Adversary*. The “covered company” operating the website or application must also be “controlled by a foreign adversary,” meaning it is “headquartered in, has its principal place of business in, or is organized under the laws” of a “foreign adversary country,” which currently includes China, North Korea, Russia, and Iran. Sec. 2(g)(1)(A), (g)(4); *see also* 10 U.S.C. § 4872(d)(2). A company may also be “controlled by a foreign adversary” if persons domiciled in any of the

specified countries (*i.e.*, China, Iran, Russia, or North Korea) directly or indirectly own at least 20 percent of the company. Sec. 2(g)(1)(B).

c. *Not Exempt under Sec. 2(g)(2)(B).* But Congress specifically exempted from the term “covered company” any “entity that operates” a website or application “whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.” An entity that operates a single website or application of this nature thus cannot be a “covered company,” even if it is “controlled by a foreign adversary,” poses a significant national security risk, and separately operates an application whose primary purpose is anything other than allowing users to post reviews. Sec. 2(g)(2)(B).

d. *Presidential Determination, Notice and Report, and Judicial Review.* Finally, the President must determine that such a company presents “a significant threat to the national security of the United States.” Sec. 2(g)(3)(B)(ii). Before making such a determination, the President must

issue public notice proposing the determination and then provide a public report to Congress describing “the specific national security concern involved,” supplemented by a classified annex, and also explain “what assets would need to be divested to execute a qualified divestiture.” *Id.* These presidential determinations are then subject to judicial review. Sec. 3(a).

35. Section 2(c) exempts a “foreign adversary controlled application[]” from the Act’s prohibitions if the company that operates the application executes a “qualified divestiture.” Sec. 2(c). The President must determine that such divestiture would (1) “result in the relevant covered company no longer being controlled by a foreign adversary,” and (2) “preclude[] the establishment or maintenance of any operational relationship” between the application’s U.S. operations and any formerly affiliated entities that are controlled by a foreign adversary, including “any cooperation with respect to the operation of a content recommendation algorithm.” Sec. 2(c), (g)(6). As noted above, the Act’s broad definition of “controlled by a foreign adversary” includes, among other things, any entity organized under the laws of a “foreign adversary



country,” or any entity in which a foreign person domiciled in a foreign adversary country holds at least a 20 percent ownership stake. Sec. 2(g)(1), (3)(B)(i), (4).

36. The prohibition on providing Internet hosting and mobile application store services to TikTok and other ByteDance applications takes effect 270 days after enactment. Sec. 2(a)(2)(A). The President may extend this deadline, but only for 90 days maximum, and only if the President certifies to Congress that a path to executing a qualified divestiture has been identified, evidence of significant progress toward executing that qualified divestiture has been produced, and the relevant binding legal agreements to enable execution of the qualified divestiture are in place.

37. “Before the date on which [this] prohibition” takes effect, Petitioners are required to provide, upon request by any U.S. user of any of their applications, “all the available data related to the account of such user with respect to such application.” Sec. 2(b).<sup>10</sup>

---

<sup>10</sup> Because Section 2(b)’s data portability requirement applies “[b]efore” the prohibition under Section 2(a) takes effect, it cannot be “given effect” without Section 2(a) for purposes of Section 2(e)(1) of the Act, which provides that “[i]f any provision of this section or the application of this

38. Because the Act lacks any legislative findings or a statement of purpose, Petitioners and the more than 170 million American monthly users of TikTok are left to scrutinize statements from individual Members of Congress and other sources to try to discern any purported justification for this extraordinary intrusion on free speech rights. Based on these sources, it appears at least some Members of Congress sought to address “two threats” that could emerge from foreign ownership of communications platforms.<sup>11</sup>

39. *First*, they may have sought to protect U.S. users’ “data security.”<sup>12</sup> According to the House Committee Report for an earlier version of the Act, mobile applications, including those that are not

---

section to any person or circumstance is held invalid, the invalidity shall not affect the other provisions or applications of this section that can be given effect without the invalid provision or application.” Because Section 2(a) violates the Constitution for the reasons set forth herein, Section 2(b) is accordingly “not operative in the absence of the unconstitutional provision.” *Barr v. Am. Ass’n of Pol. Consultants, Inc.*, 140 S. Ct. 2335, 2352 n.9 (2020).

<sup>11</sup> Jane Coaston, *What the TikTok Bill Is Really About, According to a Leading Republican*, N.Y. Times (Apr. 1, 2024), <https://perma.cc/BL32-786X> (quoting the Act’s original sponsor, Rep. Mike Gallagher).

<sup>12</sup> *Id.*

controlled by foreign adversaries, can “collect vast amounts of data on Americans.”<sup>13</sup> The House Committee Report expressed a concern that such data could be used by a foreign adversary to “conduct espionage campaigns,” such as by tracking specific individuals.<sup>14</sup>

40. *Second*, others in Congress appear to have been motivated by a “greater concern”: an alleged “propaganda threat.”<sup>15</sup> One proponent of the Act stated that communications applications could be used to “push misinformation, disinformation, and propaganda on the American public.”<sup>16</sup> Another supporter claimed in the House Select Committee press release accompanying the bill’s introduction that “[TikTok] is . . . poisoning the minds of our youth every day on a massive scale.”<sup>17</sup>

---

<sup>13</sup> H.R. Comm. on Energy & Com., *Protecting Americans from Foreign Adversary Controlled Applications Act*, H.R. Rep. No. 118-417 at 2 (2024) (hereinafter the “House Committee Report”).

<sup>14</sup> *Id.*

<sup>15</sup> Coaston, *supra* n.11 (quoting Rep. Gallagher).

<sup>16</sup> House Committee Report at 2.

<sup>17</sup> Press Release, U.S. House Select Comm. on Strategic Competition Between the U.S. and the Chinese Communist Party, Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans From Foreign Adversary Controlled Applications, Including TikTok (Mar. 5, 2024), <https://perma.cc/KC5T-6AX3>.

**E. Congress Disregarded Alternatives to Banning TikTok, Such as the National Security Measures Petitioners Negotiated with the Executive Branch.**

41. Petitioners have demonstrated a commitment to addressing both of those concerns without the need to resort to the drastic, unconstitutional step of shuttering one of the most widely used forums for speech in the United States. The 90-page draft National Security Agreement that Petitioners developed with CFIUS would, if implemented, provide U.S. TikTok users with protections more robust than those employed by any other widely used online platform in the industry.

42. The draft National Security Agreement contains several means of ensuring data security without banning TikTok. All protected U.S. user data (as defined in the National Security Agreement) would be safeguarded in the United States under a special corporate structure: TikTok U.S. Data Security (a new subsidiary of TikTok Inc.). A special board, with Security Directors whose appointment would be subject to the U.S. government's approval, would oversee TikTok U.S. Data Security, and in turn exclude ByteDance and all of its other subsidiaries and affiliates from such responsibilities. Further separation between the

U.S. TikTok business and ByteDance subsidiaries and affiliates, including TikTok in the rest of the world, would be achieved by appointing a U.S.-government-approved Security Director to the board of TikTok Inc. Protected U.S. user data would be stored in the cloud environment of a U.S.-government-approved partner, Oracle Corporation, with access to such data managed by TikTok U.S. Data Security.

43. The draft Agreement would also protect against the concern about content manipulation and propaganda. Multiple layers of protection address concerns related to content available on the TikTok platform, including ensuring that all content moderation — both human and algorithmic — would be subject to third-party verification and monitoring. The concern about content manipulation would also be addressed by securing all software code through Oracle Corporation, a U.S. trusted technology provider. The TikTok U.S. platform and application would be deployed through the Oracle cloud infrastructure and subject to source code review and vetting by Oracle with another U.S.-government-approved third party responsible for conducting security inspections. As part of this process, Oracle and third parties

approved by CFIUS would conduct independent inspections of the TikTok recommendation engine.

44. The draft Agreement also includes strict penalties for noncompliance, including a “shut-down option,” giving the government the authority to suspend TikTok in the United States in response to specified acts of noncompliance. The Agreement also provides significant monetary penalties and other remedies for noncompliance.

45. Although the government has apparently abandoned the draft National Security Agreement, Petitioners have not. TikTok Inc. has begun the process of voluntarily implementing the National Security Agreement’s provisions to the extent it can do so without the U.S. government’s cooperation, including by incorporating and staffing the TikTok U.S. Data Security entity, and by partnering with Oracle Corporation on the migration of the U.S. platform and protected U.S. user data to Oracle’s cloud environment.

46. To date, Petitioners have spent more than \$2 billion to implement these measures and resolve the very concerns publicly expressed by congressional supporters of the Act — all without the overbroad and unconstitutional method of an outright ban.

### **Grounds On Which Relief Is Sought**

Petitioners seek review of the constitutionality of the Act on grounds that include, without limitation, the following.

#### **Ground 1: Violation of the First Amendment**

47. The First Amendment to the U.S. Constitution provides that “Congress shall make no law . . . abridging the freedom of speech.” U.S. Const., amend. I.

48. By banning all online platforms and software applications offered by “TikTok” and all ByteDance subsidiaries, Congress has made a law curtailing massive amounts of protected speech. Unlike broadcast television and radio stations, which require government licenses to operate because they use the public airwaves, the government cannot, consistent with the First Amendment, dictate the ownership of newspapers, websites, online platforms, and other privately created speech forums.

49. Indeed, in the past, Congress has recognized the importance of protecting First Amendment rights, even when regulating in the interest of national security. For example, Congress repeatedly amended IEEPA — which grants the President broad authority to address national

emergencies that pose “unusual and extraordinary threat[s]” to the country — to expand protections for constitutionally protected materials. 50 U.S.C. §§ 1701–02. Accordingly, under IEEPA, the President does not have the authority to even *indirectly* regulate “personal communication” or the importation or exportation “of any information or informational materials,” *id.* § 1702(b)(1), (3) — limitations that are necessary “to prevent the statute from running afoul of the First Amendment,” *Amirnazmi*, 645 F.3d at 585. Yet Congress has attempted to sidestep these statutory protections aimed at protecting Americans’ constitutional rights, preferring instead to simply enact a *new* statute that tries to avoid the constitutional limitations on the government’s existing statutory authority. Those statutory protections were evidently seen as an impediment to Congress’s goal of banning TikTok, so the Act dispensed with them.

50. The Act’s alternative to a ban — a so-called “qualified divestiture” — is illusory to the point of being no alternative at all. As explained above, divesting TikTok Inc.’s U.S. business and completely severing it from the globally integrated platform of which it is a part is not commercially, technologically, or legally feasible.



51. The Act will therefore have the effect of shutting down TikTok in the United States, a popular forum for free speech and expression used by over 170 million Americans each month. And the Act will do so based not on *any* proof of a compelling interest, but on speculative and analytically flawed concerns about data security and content manipulation — concerns that, even if grounded in fact, could be addressed through far less restrictive and more narrowly tailored means.

52. ***Petitioners’ protected speech rights.*** The Act burdens TikTok Inc.’s First Amendment rights — in addition to the free speech rights of millions of people throughout the United States — in two ways.

53. *First*, Petitioner TikTok Inc. has a First Amendment interest in its editorial and publishing activities on TikTok. *See Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos.*, 515 U.S. 557, 570 (1995). TikTok “is more than a passive receptacle or conduit for news, comment, and advertising” of others; TikTok Inc.’s “choice of material” to recommend or forbid “constitute[s] the exercise of editorial control and judgment” that is protected by the First Amendment. *Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241, 258 (1974); *see also Alario v. Knudsen*,

— F. Supp. 3d —, 2023 WL 8270811, at \*6 (D. Mont. Nov. 30, 2023) (recognizing TikTok Inc.’s First Amendment editorial rights).

54. As the government itself has acknowledged, “[w]hen [social media] platforms decide which third-party content to present and how to present it, they engage in expressive activity protected by the First Amendment because they are creating expressive compilations of speech.” Br. for United States as Amicus Curiae at 12–13, *Moody v. NetChoice LLC*, No. 22-277 (U.S.), 2023 WL 8600432; *see also id.* at 18–19, 25–26.

55. *Second*, TikTok Inc. is among the speakers whose expression the Act prohibits. TikTok Inc. uses the TikTok platform to create and share its own content about issues and current events, including, for example, its support for small businesses, Earth Day, and literacy and education.<sup>18</sup> When TikTok Inc. does so, it is engaging in core speech protected by the First Amendment. *See Sorrell v. IMS Health Inc.*, 564

---

<sup>18</sup> TikTok (@tiktok), TikTok, <https://www.tiktok.com/t/ZTL9QsTYs/> (last visited May 6, 2024); TikTok (@tiktok), TikTok, <https://www.tiktok.com/t/ZTL9QbSHv/> (last visited May 6, 2024); TikTok (@tiktok), TikTok, <https://www.tiktok.com/t/ZTL9QXE7R/> (last visited May 6, 2024).

U.S. 552, 570 (2011); *NetChoice, LLC v. Att’y Gen., Fla.*, 34 F.4th 1196, 1210 (11th Cir. 2022), *cert. granted*, 144 S. Ct. 478 (2023). The Act precludes TikTok Inc. from expressing itself over that platform.

56. Even if the U.S. TikTok platform could be divested, which it cannot for the reasons explained above, TikTok Inc.’s protected speech rights would still be burdened. Because the Act appears to conclusively determine that any application operated by “TikTok” — a term that Congress presumably meant to include TikTok Inc. — is a foreign adversary controlled application, Sec. 2(g)(3)(A), the President appears to lack the power to determine that a TikTok Inc.-owned application is “no longer being controlled by a foreign adversary” and has no “operational relationship” with “formerly affiliated entities that are controlled by a foreign adversary,” Sec. 2(g)(6)(A) & (B). The Act therefore appears to conclusively eliminate TikTok Inc.’s ability to speak through its editorial and publishing activities and through its own account on the TikTok platform.

57. For similar reasons, the Act burdens the First Amendment rights of other ByteDance subsidiaries to reach their U.S. user audiences,

since those companies are likewise prohibited from speaking and engaging in editorial activities on other ByteDance applications.

58. ***The Act is subject to strict scrutiny.*** The Act’s restrictions on Petitioners’ First Amendment rights are subject to strict scrutiny for three independent reasons.

59. *First*, the Act represents a content- and viewpoint-based restriction on protected speech. The Act discriminates on a content basis because it exempts platforms “whose primary purpose” is to host specific types of content: “product reviews, business reviews, or travel information and reviews.” Sec. 2(g)(2)(B). The Act thus “distinguish[es] favored speech” — *i.e.*, speech concerning travel information and business reviews — “from disfavored speech” — *i.e.*, all other types of speech, including particularly valuable speech like religious and political content. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 643 (1994).

60. The Act also discriminates on a viewpoint basis because it appears to have been enacted at least in part because of concerns over the viewpoints expressed in videos posted on TikTok by users of the platform. For example, the House Committee Report asserted, without supporting evidence, that TikTok “can be used by [foreign adversaries] to

... push misinformation, disinformation, and propaganda on the American public”<sup>19</sup> — a concern that in any event could be raised about any platform for user-generated content. *See infra* ¶¶ 82, 87. Similarly, Rep. Raja Krishnamoorthi, who co-sponsored the Act, expressed the unsubstantiated concern that “the platform continued to show dramatic differences in content relative to other social media platforms.”<sup>20</sup>

61. *Second*, the Act discriminates between types of speakers. As explained above, TikTok Inc. is a protected First Amendment speaker with respect to the TikTok platform. The Act facially discriminates between TikTok Inc. and other speakers depending on the “primary purpose” of the platforms they operate. Any application offered by Petitioners is automatically deemed a “foreign adversary controlled application,” without any exclusions or exceptions. Sec. 2(g)(3)(A). By contrast, any other company’s application can be deemed a “foreign adversary controlled application” only if the company does not operate a

---

<sup>19</sup> House Committee Report at 2.

<sup>20</sup> Sapna Maheshwari, David McCabe & Annie Karni, *House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App*, N.Y. Times (Mar. 13, 2024), <https://perma.cc/Z7UE-WYH6>.

website or application “whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.” Sec. 2(g)(2)(B). The Act thus favors speakers that *do* offer such websites or applications over speakers that do not.

62. Moreover, the Act singles out TikTok Inc. and other subsidiaries of ByteDance for unique disfavor in other ways. Whereas *other* companies with ownership in a country deemed a “foreign adversary” become subject to the Act’s restrictions only upon a presidential determination that the company poses “a significant threat to the national security of the United States,” Sec. 2(g)(3)(B), ByteDance Ltd. and its subsidiaries are automatically subject to the Act’s draconian restrictions by fiat, Sec. 2(g)(3)(A). The standard and process that the Act specifies for every other company likely fall short of what is required by the First Amendment and other applicable constitutional protections, but TikTok Inc. and ByteDance have been singled out for a dramatically different, even more clearly unconstitutional regime — with no public notice, no process for a presidential determination that there is a significant national security threat, no justification of that determination by a public report and submission of classified evidence to Congress, and

no judicial review for statutory and constitutional sufficiency based on the reasons set forth in the presidential determination. The Act also draws a speaker-based distinction insofar as it specifically names ByteDance Ltd. and TikTok, and also exempts applications with fewer than 1 million monthly users (except if those applications are operated by ByteDance Ltd. or TikTok). Sec. 2(g)(2)(A)(ii), (3)(A).

63. A statutory restriction targeting specific classes of speakers is subject to strict scrutiny. *See United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 812 (2000) (“Laws designed or intended to suppress or restrict the expression of certain speakers contradict basic First Amendment principles.”). And that is especially true when, as here, the Act singles out Petitioners by name for uniquely disfavored treatment and congressional statements indicate that the Act targets Petitioners in part because of concerns about the content on TikTok. Because the Act “target[s]” both “speakers and their messages for disfavored treatment,” strict scrutiny review is required. *Sorrell*, 564 U.S. at 565; *see also Turner*, 512 U.S. at 658–60.

64. *Third*, the Act is subject to strict scrutiny as an unlawful prior restraint. The Supreme Court has “consistently” recognized in a “long

line” of cases that government actions that “deny use of a forum in advance of actual expression” or forbid “the use of public places [for plaintiffs] to say what they wanted to say” are prior restraints. *Se. Promotions, Ltd. v. Conrad*, 420 U.S. 546, 552–53 (1975). “[P]rior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights.” *Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976). The Act suppresses speech in advance of its actual expression by prohibiting all U.S. TikTok users — including Petitioner TikTok Inc. — from communicating on the platform. *See Backpage.com, LLC v. Dart*, 807 F.3d 229 (7th Cir. 2015) (defendant’s conduct restricting the operator of classified advertising website was a prior restraint); *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 418–19 (1971) (ban on distributing leaflets a prior restraint); *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912, 926 (N.D. Cal. 2020) (ban on communications application a prior restraint). The same is true of other ByteDance subsidiaries and their platforms. Such restrictions “bear[] a heavy presumption against [their] constitutional validity.” *Se. Promotions*, 420 U.S. at 558.



65. *The Act fails strict scrutiny because it does not further a compelling interest.* Strict scrutiny “requires the Government to prove that the restriction [1] furthers a compelling interest and [2] is narrowly tailored to achieve that interest.” *Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (numerical alterations added). “If a less restrictive alternative would serve the Government’s purpose, the legislature must use that alternative.” *Playboy*, 529 U.S. at 813. The Act fails on both counts.

66. The Act does not further a compelling interest. To be sure, national security is a compelling interest, but the government must show that the Act furthers that interest. To do so, the government “must do more than simply posit the existence of the disease sought to be cured.” *Turner*, 512 U.S. at 664 (plurality op.). Rather, it “must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.” *Id.*

67. Congress itself has offered nothing to suggest that the TikTok platform poses the types of risks to data security or the spread of foreign propaganda that could conceivably justify the Act. The Act is devoid of

any legislative findings, much less a demonstration of specific harms that TikTok supposedly poses in either respect, even though the platform was first launched in 2017.

68. The statements of congressional committees and individual Members of Congress during the hasty, closed-door legislative process preceding the Act's enactment confirm that there is at most speculation, not "evidence," as the First Amendment requires. Instead of setting out evidence that TikTok is *actually* compromising Americans' data security by sharing it with the Chinese government or spreading pro-China propaganda, the House Committee Report for an earlier version of the Act relies repeatedly on speculation that TikTok *could* do those things. *See, e.g.*, House Committee Report at 6 (TikTok could "*potentially* [be] allowing the CCP 'to track the locations of Federal employees and contractors'") (emphasis added) (quoting Exec. Order 13,942, 85 Fed. Reg. 48637, 48637 (Aug. 6, 2020)); *id.* at 8 (discussing "the *possibility* that the [CCP] could use [TikTok] to control data collection on millions of users") (emphasis added); *id.* ("TikTok has sophisticated capabilities that create the *risk* that [it] can . . . suppre[ss] statements and news that the PRC deems negative") (emphasis added). Speculative risk of harm is simply

not enough when First Amendment values are at stake. These risks are even more speculative given the other ways that the Chinese government could advance these asserted interests using a variety of intelligence tools and commercial methods. *See infra* ¶¶ 85–87.

69. The conjectural nature of these concerns are further underscored by President Biden’s decision to continue to maintain a TikTok account for his presidential campaign even after signing the Act into law.<sup>21</sup> Congressional supporters of the Act have also maintained campaign accounts on TikTok.<sup>22</sup> This continued use of TikTok by President Biden and Members of Congress undermines the claim that the platform poses an actual threat to Americans.

70. Further, even if the government *could* show that TikTok or another ByteDance-owned application “push[es] misinformation, disinformation, and propaganda on the American public,” House

---

<sup>21</sup> Monica Alba, Sahil Kapur & Scott Wong, *Biden Campaign Plans to Keep Using TikTok Through the Election*, NBC News (Apr. 24, 2024), <https://perma.cc/QPQ5-RVAD>.

<sup>22</sup> Tom Norton, *These US Lawmakers Voted for TikTok Ban But Use It Themselves*, Newsweek (Apr. 17, 2024), <https://perma.cc/AQ5F-N8XQ>. At least one Member created a TikTok account after the Act was enacted. *See* <https://perma.cc/L3GT-7529>.

Committee Report at 2, the government would still lack a compelling interest in preventing Americans from hearing disfavored speech generated by TikTok users and shared on the platform just because the government considers it to be foreign “propaganda.” See *Lamont v. Postmaster Gen. of U.S.*, 381 U.S. 301, 305 (1965).

71. The Act also offers no support for the idea that other applications operated by subsidiaries of ByteDance Ltd. pose national security risks. Indeed, the legislative record contains no meaningful discussion of *any* ByteDance-owned application other than TikTok — let alone evidence “proving” that those other applications pose such risks. *Reed*, 576 U.S. at 171.

72. The Act also provides neither support nor explanation for subjecting Petitioners to statutory disqualification by legislative fiat while providing every other platform, and users of other platforms, with a process that includes a statutory standard for disqualification, notice, a reasoned decision supported by evidence, and judicial review based on those specified reasons. Only Petitioners are subjected to a regime that has no notice and no reasoned decision supported by evidence — opening the door to, among other things, post-hoc arguments that may not have

been the basis for the government action. The Supreme Court recently explained that the requirement of a “reasoned explanation” is “meant to ensure that [the government] offer[s] genuine justifications for important decisions, reasons that can be scrutinized by courts and the interested public. Accepting contrived reasons would defeat the purpose of the enterprise.” *Dep’t of Com. v. New York*, 139 S. Ct. 2551, 2576 (2019). Depriving Petitioners of those protections imposes a dramatically heavier burden on the free speech rights of Petitioners and TikTok users that is wholly unjustified and certainly not supported by a compelling interest.

73. ***The Act also fails strict scrutiny because it is not narrowly tailored.*** “Even where questions of allegedly urgent national security . . . are concerned,” the government must show that “the evil that would result from the [restricted speech] is both great and certain and cannot be mitigated by less intrusive measures.” *CBS, Inc. v. Davis*, 510 U.S. 1315, 1317 (1994). To satisfy narrow tailoring, the Act must represent the least restrictive means to further the government’s asserted data security and propaganda interests, *Sable Commc’ns of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989), and be neither over- nor under-

inclusive, *Ark. Writers' Project, Inc. v. Ragland*, 481 U.S. 221, 232 (1987).

The Act fails in each of these respects.

74. The Act opts for a wholesale prohibition on Petitioners offering online applications in lieu of a multitude of less restrictive measures it could have taken instead. As discussed above, Petitioners have been involved in negotiations with CFIUS since 2019 over a package of measures that would resolve the government's concerns about data security and purported propaganda related to TikTok. The terms of that negotiated package are far less restrictive than an outright ban. The negotiations have resulted in the draft National Security Agreement, which TikTok Inc. is *already* in the process of voluntarily implementing to the extent it can do so without government action. That initiative includes a multi-billion-dollar effort to create a new TikTok U.S. subsidiary devoted to protecting U.S. user data and have U.S.-based Oracle Corporation store protected U.S. TikTok user data in the United States, run the TikTok recommendation system for U.S. users, and inspect TikTok's source code for security vulnerabilities.

75. If executed by the government, the National Security Agreement would also give CFIUS a "shut-down option" to suspend

TikTok in the United States in response to specified acts of noncompliance. The government has never meaningfully explained why the National Security Agreement (a far less restrictive alternative to an outright, total ban) is insufficient to address its stated concerns about data security and propaganda.

76. Even if the government's dissatisfaction with the draft National Security Agreement were valid (despite the government never explaining why the agreement that the government itself negotiated is unsatisfactory), the CFIUS process in which Petitioners have participated in good faith is geared toward finding any number of other less restrictive alternatives to an outright, total ban. The CFIUS member agencies could return to working with Petitioners to craft a solution that is tailored to meet the government's concerns and that is commercially, technologically, and legally feasible. Yet the government has not explained why the CFIUS process is not a viable alternative.

77. There are also a wide range of other less restrictive measures that Congress could have enacted. While many of these measures are themselves unjustified as applied to Petitioners, they nevertheless illustrate that the Act does not select the least restrictive means to

further the national security goals that appear to have motivated it. For example, Congress could have addressed some members' stated concern about TikTok allegedly "track[ing] the locations of Federal employees and contractors"<sup>23</sup> by expanding the existing ban on government-owned devices to cover personal devices of federal employees and contractors. Or Congress could have enacted legislation to regulate TikTok's access to certain features on users' devices — measures the Department of Homeland Security identified in 2020 as potential mitigations to "reduce the national security risks associated with" TikTok.<sup>24</sup>

78. Of course, Congress could also have decided not to single out a single speech platform (TikTok) and company (ByteDance Ltd.), and instead pursued any number of industry-wide regulations aimed at addressing the industry-wide issues of data security and content integrity. Congress could have enacted a data protection law governing transfers of Americans' sensitive data to foreign countries, similar to the

---

<sup>23</sup> House Committee Report at 6.

<sup>24</sup> Cybersecurity and Infrastructure Agency, Critical Infrastructure Security and Resilience Note, Appendix B: Department of Homeland Security TikTok and WeChat Risk Assessment 4 (Sept. 2, 2020).



strategy President Biden is currently pursuing through executive order.<sup>25</sup> Indeed, Congress *did* enact such a data-transfer law — the similarly named “Protecting Americans’ Data from Foreign Adversaries Act of 2024” — as the *very next division* of the legislation that contains the Act. Yet it chose to prohibit only “data broker[s]” from “mak[ing] available personally identifiable sensitive data of a United States individual to any foreign adversary country or . . . any entity that is controlled by a foreign adversary.” H.R. 815, div. I, § 2(a), 118th Cong., Pub. L. No. 118-50 (Apr. 24, 2024).

79. There are also models for industry-wide regulation that Congress could have followed from other jurisdictions. For example, the European Union’s Digital Services Act requires certain platforms to make disclosures about their content-moderation policies and to provide regulators and researchers with access to their data so those researchers can assess if the platforms are systemically promoting or suppressing

---

<sup>25</sup> See Exec. Order 14,117, 89 Fed. Reg. 15421 (Mar. 1, 2024).

content with particular viewpoints.<sup>26</sup> Congress pursued none of these alternatives.

80. Congress did not even provide Petitioners with the process and fact-finding protections that the Act extends to all other companies — protections which themselves likely fall short of what the Constitution mandates. Other companies receive prior notice, followed by a presidential determination of (and public report on) the national security threat posed by the targeted application, and the submission to Congress of classified evidence supporting that determination, Sec. 2(g)(3)(B), which then is subject to judicial review based on the actual reasons for the decision, not post hoc rationalizations.

81. Because Congress failed to try any of these less restrictive measures, or at a minimum to explain why these alternatives would not address the government's apparent concerns, the Act is not narrowly tailored.

82. ***The Act independently fails strict scrutiny because it is both under- and over-inclusive.*** The Act is under-inclusive because it

---

<sup>26</sup> EU Reg. 2022/2065 arts. 15, 40(4), 42(2).

ignores the many ways in which other companies — both foreign and domestic — can pose the same risks to data security and promotion of misinformation supposedly posed by Petitioners. The government “cannot claim” that banning some types of foreign owned applications is “necessary” to prevent espionage and propaganda “while at the same time” allowing other types of platforms and applications that may “create the same problem.” *Reed*, 576 U.S. at 172. Put differently, the Act’s “[u]nderinclusiveness raises serious doubts about whether the government is in fact pursuing the interest it invokes, rather than disfavoring a particular speaker or viewpoint.” *Brown v. Ent. Merchants Ass’n*, 564 U.S. 786, 802 (2011).

83. Most glaringly, the Act applies only to Petitioners and certain other platforms that allow users to generate and view “text, images, videos, real-time communications, or similar content.” Sec. 2(g)(2)(A). The Act’s coverage is thus triggered not by whether an application collects users’ *data*, but whether it shows them “*content*.” Accordingly, there is no necessary relationship between the Act’s scope and Congress’s apparent concern with risks to Americans’ data security, which could

equally be posed by personal finance, navigation, fitness, or many other types of applications.

84. The Act also singles out Petitioners by exempting all other companies that operate any website or application “whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.” Sec. 2(g)(2)(B). But the Act does not explain why such applications, when (i) “foreign adversary controlled” under the Act’s broad definition; and (ii) determined by the President to be a significant national security threat, could not likewise be used to collect data from Americans — such as Americans’ location information — or to spread misinformation. Nor does the Act explain why an entire *company* presents no threat simply because it operates a *single* website or application the “primary purpose” of which is posting “product reviews, business reviews, or travel information and reviews.” Sec. 2(g)(2)(B). The Act’s differential treatment of this favored category of websites and applications also disregards the fact that there is voluminous content on TikTok containing product reviews, business reviews, and travel information and reviews. Yet TikTok and all ByteDance applications are ineligible for this exclusion.

85. More broadly, the Act ignores the reality that much of the data collected by TikTok is no different in kind from the data routinely collected by other applications and sources in today's online world, including by American companies like Google, Snap, and Meta. The Act also ignores that foreign countries, including China, can obtain such information on Americans in other ways — such as through open-source research and hacking operations.

86. Likewise, the House Committee Report on an earlier version of the Act speculates that allowing source code development in China “potentially exposes U.S. users to malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development.”<sup>27</sup> But those supposed risks arise for each of the many American companies that employ individuals in China to develop code. The Act, however, does not seek to regulate, much less prohibit, all online applications offered by companies that have offices in China or that otherwise employ Chinese nationals as software developers.<sup>28</sup>

---

<sup>27</sup> House Committee Report at 5.

<sup>28</sup> See, e.g., Karen Freifeld & Jonathan Stempel, *Former Google Engineer*

87. Nor does the Act seek to cut off numerous other ways that Americans could be exposed to foreign propaganda. For instance, the Act leaves foreign nationals (and even adversarial governments themselves) free to operate cable television networks in the United States, spread propaganda through accounts on other online platforms that enable the sharing of user-generated content, or distribute copies of state-run newspapers physically or over the Internet (including by software applications) in the United States.<sup>29</sup>

---

*Indicted for Stealing AI Secrets to Aid Chinese Companies*, Reuters (Mar. 6, 2024), <https://perma.cc/6LYE-64J6>.

<sup>29</sup> The U.S. government has recognized that foreign government propaganda is an industry-wide challenge for online platforms. *See, e.g.*, Nat'l Intel. Council, *Declassified Intelligence Community Assessment, Foreign Threats to the 2020 US Federal Elections* (Mar. 10, 2021), <https://perma.cc/VD3Y-VXSB>. YouTube, for example, added disclaimers to certain channels that were reportedly being used to spread disinformation on behalf of the Russian government. Paresh Dave & Christopher Bing, *Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels - Researchers*, Reuters (June 7, 2019), <https://perma.cc/2BEJ-VKGW>. Like others in the industry, TikTok publishes transparency reports on attempts by users to use the platform for government propaganda purposes. *See* TikTok, *Countering Influence Operations* (last visited May 6, 2024), <https://perma.cc/AB39-S8FJ>.

88. The Act is also over-inclusive because it applies to other ByteDance Ltd.-owned applications that Congress has not shown — and could not possibly prove — pose the risks the Act apparently seeks to address.

89. ***At a minimum, the Act fails intermediate scrutiny.*** Even if strict scrutiny did not apply, the Act would still fail intermediate scrutiny as a time, place, and manner restriction: the Act prohibits speech activity on TikTok at all times, in all places, and in all manners anywhere across the United States. To pass intermediate scrutiny, a law must be “narrowly tailored to serve a significant governmental interest.” *McCullen v. Coakley*, 573 U.S. 464, 486 (2014). This means that it must not “burden substantially more speech than is necessary to further the government’s legitimate interests,” *Turner*, 512 U.S. at 661–62, and “leave open ample alternative channels for communication of the information,” *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984).

90. For many of the same reasons the Act cannot satisfy strict scrutiny, it also cannot satisfy intermediate scrutiny:

91. As discussed *supra* ¶¶ 67–69, the government has failed to establish that its apparent data security and propaganda concerns with TikTok are non-speculative. And as discussed *supra* ¶¶ 73–81, the Act burdens substantially more speech than necessary because there are many less restrictive alternatives Congress could have adopted to address any legitimate concerns. The Act also fails intermediate scrutiny because it “effectively prevents” TikTok Inc. “from reaching [its] intended audience” and thus “fails to leave open ample alternative means of communication.” *Edwards v. City of Coeur d’Alene*, 262 F.3d 856, 866 (9th Cir. 2001).

92. Regardless of the level of scrutiny, the Act violates the First Amendment for two additional reasons.

93. ***The Act forecloses an entire medium of expression.*** First, by banning TikTok in the United States, the Act “foreclose[s] an entire medium of expression.” *City of Ladue v. Gilleo*, 512 U.S. 43, 56 (1994). A “long line of Supreme Court cases indicates that such laws are almost *never* reasonable.” *Anderson v. City of Hermosa Beach*, 621 F.3d 1051, 1064–65 (9th Cir. 2010).



94. ***The Act is constitutionally overbroad.*** Second, the Act is facially overbroad. A law is “overbroad if a substantial number of its applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *United States v. Stevens*, 559 U.S. 460, 473 (2010) (citation omitted). Here, for example, the government has never contended that *all* — or even *most* — of the content on TikTok (or any other ByteDance-owned application) represents disinformation, misinformation, or propaganda. Yet the Act shuts down all speech on ByteDance-owned applications at all times, in all places, and in all manners. That is textbook overbreadth. *See, e.g., Bd. of Airport Comm’rs v. Jews for Jesus, Inc.*, 482 U.S. 569, 574–75 (1987).

### **Ground 2: Unconstitutional Bill of Attainder**

95. The Act is an unconstitutional bill of attainder.

96. Article I of the U.S. Constitution prohibits Congress from passing any bill of attainder. U.S. Const. art. I § 9, cl. 3 (“No Bill of Attainder or ex post facto Law shall be passed.”). A bill of attainder is “legislative punishment, of any form or severity, of specifically designated persons or groups.” *United States v. Brown*, 381 U.S. 437, 447 (1965). The protection against bills of attainder is “an implementation of

the separation of powers, a general safeguard against legislative exercise of the judicial function, or more simply — trial by legislature.” *Id.* at 442.

97. By singling out Petitioners for legislative punishment, the Act is an unconstitutional bill of attainder.

98. The Act inflicts “pains and penalties” that historically have been associated with bills of attainder. *See Nixon v. Adm’r of Gen. Servs.*, 433 U.S. 425, 474 (1977). Historically, common “pains and penalties” included “punitive confiscation of property by the sovereign” and “a legislative enactment barring designated individuals or groups from participation in specified employments or vocations,” among others. *Id.* As described above, the Act confiscates Petitioners’ U.S. businesses by forcing ByteDance to shutter them within 270 days or sell on terms that are not commercially, technologically, or legally feasible. *See supra* ¶¶ 26–29. For the same reason, the Act bars Petitioners from operating in their chosen line of business.

99. “[V]iewed in terms of the type and severity of burdens imposed” on Petitioners, the Act’s treatment of Petitioners cannot “reasonably . . . be said to further nonpunitive legislative purposes.” *Nixon*, 433 U.S. at 475–76. The Act transforms Petitioners into a “vilified

class” by explicitly prohibiting their current and future operations in the United States, without qualification or limitation, but does not extend the same treatment to other similarly situated companies. *Foretich v. United States*, 351 F.3d 1198, 1224 (D.C. Cir. 2003).

100. Moreover, in light of the less restrictive alternatives discussed above, there is no justification for automatically barring Petitioners’ current and future operations in the United States (or those of its subsidiaries or successors) in perpetuity without providing them a meaningful opportunity to take corrective action. *See Kaspersky Lab, Inc. v. U.S. Dep’t of Homeland Sec.*, 909 F.3d 446, 456 (D.C. Cir. 2018). Indeed, the Act imposes this punishment uniquely on Petitioners *without* the process, and presidential determination of a significant national security threat, that Congress has afforded to everyone else. Expressly singling out Petitioners for these punitive burdens while at the same time adopting a statutory standard and decision-making process applicable to every other entity makes clear that Petitioners are subjected to a prohibited legislatively imposed punishment.

101. Moreover, while Petitioners can avoid the Act’s prohibitions only via a wholesale divestment, all other companies — even those with

Chinese ownership and determined by the President to present a “significant threat” to U.S. national security — can avoid prohibition simply by operating a website or an application “whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.” Sec. 2(g)(2)(b).

102. Indeed, any other “adversary-controlled” company that operates an application exactly like TikTok, but *also* operates a website the primary purpose of which is to post product reviews, is left untouched, leaving a ready path for any company but those affiliated with Petitioners to circumvent the Act’s prohibitions altogether. For all practical purposes, then, the Act applies to just one corporate group — it is a “TikTok bill,” as congressional leaders have described it.<sup>30</sup>

103. For all of these reasons, the Act constitutes an unconstitutional bill of attainder.

---

<sup>30</sup> Rachel Dobkin, *Mike Johnson’s Letter Sparks New Flood of Republican Backlash*, Newsweek (Apr. 17, 2024), <https://perma.cc/Z5HD-7UVU> (quoting letter from Speaker Johnson referencing the “TikTok bill”); Senator Chuck Schumer, Majority Leader, to Colleagues (Apr. 5, 2024), <https://perma.cc/J7Q4-9PGJ> (referencing “TikTok legislation”).

### Ground 3: Violation of Equal Protection

104. The Act also violates Petitioners' rights under the equal protection component of the Fifth Amendment's Due Process Clause because it singles Petitioners out for adverse treatment without any reason for doing so.

105. *First*, the Act deems any application offered by Petitioners to be a "foreign adversary controlled application" without notice or a presidential determination. Sec. 2(g)(3)(A). By contrast, applications offered by other companies "controlled by a foreign adversary" are deemed to be "foreign adversary controlled applications" only after notice and a presidential determination that those companies present "significant threat[s]" to U.S. national security, a determination that must be supported by evidence submitted to Congress. Sec. 2(g)(2)(B); *see supra* ¶ 34(d).

106. That distinction imposes a dramatically heavier burden on Petitioners' free speech rights without any justification. The Act precludes the government from burdening the speech rights of any speakers other than Petitioners unless and until the President issues a public report on the specific national security concerns animating the

President's decision, provides support for that decision, and describes the assets requiring divestiture. Those protections ensure that the President must, at the very least, provide a detailed national security justification for his or her actions before burdening other speakers' speech — a justification that then will provide the basis for judicial review. The Act imposes none of those requirements as a precondition for burdening Petitioners' speech — it levies that burden by unexplained legislative fiat.

107. *Second*, the Act denies Petitioners the exemption available to any other company that is purportedly “controlled by a foreign adversary.” As noted, any application Petitioners offer is *ipso facto* deemed a “foreign adversary controlled application.” By contrast, other companies “controlled by a foreign adversary” are exempt from the Act's definition of a “covered company,” and thus from the Act's requirements, so long as they offer at least one application with the “primary purpose” of “allow[ing] users to post product reviews, business reviews, or travel information and reviews.” Sec. 2(g)(2)(B).

108. There is no conceivable reason for treating Petitioners differently than all other similarly situated companies. Even if Congress

had valid interests in protecting U.S. users' data and controlling what content may be disseminated through global platforms that would be advanced through the Act, there is no reason why those concerns would support a ban on Petitioners' platforms without corresponding bans on other platforms. Nor is there any rational reason why Congress would ban Petitioners' platforms while allowing any other company "controlled by a foreign adversary" — regardless of the national security threat posed by that company — to sidestep the Act's reach by simply offering an application that "allows users to post product reviews, business reviews, or travel information and reviews," but changing nothing else about the company's operations, ownership structure, or other applications.

109. By treating Petitioners differently from others similarly situated, the Act denies Petitioners the equal protection of the law.

#### **Ground 4: Unconstitutional Taking**

110. The Act effects an unlawful taking of private property without just compensation, in violation of the Fifth Amendment's Takings Clause.

111. The Takings Clause provides that "private property" shall not be "taken for public use, without just compensation." U.S. Const. amend. V, cl. 5. The Act does just that by shutting down ByteDance's

U.S. businesses or, to the extent any qualified divestiture alternative is even feasible (it is not), compelling ByteDance to sell those businesses under fire-sale circumstances that guarantee inadequate compensation.

112. Petitioners have substantial property interests in, and associated with, their and their affiliates' U.S. operations. These include not only ByteDance Ltd.'s interest in TikTok Inc. and other U.S. businesses, but also the platforms and applications themselves. *See Kimball Laundry Co. v. United States*, 338 U.S. 1, 11–13 (1949) (Takings Clause also protects losses to going-concern value of business).

113. If the Act's prohibitions take effect, they will deprive Petitioners of property protected by the Takings Clause. Absent a qualified divestiture, the Act will shutter Petitioners' businesses in the United States. And even if a qualified divestiture were feasible (it is not), any sale could be, at best, completed only at an enormous discount to the U.S. businesses' current market value, given the forced sale conditions. *See BFP v. Resol. Tr. Corp.*, 511 U.S. 531, 537 (1994) (“[M]arket value, as it is commonly understood, has no applicability in the forced-sale context; indeed, it is the very *antithesis* of forced-sale value.”).



114. Because the Act compels ByteDance “to relinquish specific, identifiable property” or forfeit “*all* economically beneficial uses,” the Act effects a per se taking. *Horne v. Dep’t of Agric.*, 576 U.S. 350, 364–65 (2015); *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1019 (1992).

115. Alternatively, the Act inflicts a regulatory taking. Even when a law does not compel the physical invasion of property or deprive the property of all economically viable use, it still effects a taking “if [it] goes too far.” *Penn. Coal Co. v. Mahon*, 260 U.S. 393, 415 (1922). In determining when a law “goes too far,” courts have typically looked to “several factors” identified in *Penn Central Transportation Co. v. City of New York*, 438 U.S. 104, 124 (1978), namely, (a) “[t]he economic impact of the regulation”; (b) “the extent to which the regulation has interfered with reasonable investment-backed expectations”; and (c) “the character of the governmental action.” The Act inflicts a regulatory taking under each of these three factors.

116. The Act does not compensate Petitioners (let alone provide just compensation) for the dispossession of their U.S. businesses. *See United States v. Miller*, 317 U.S. 369, 373 (1943). Prospective injunctive

relief is accordingly warranted. *See, e.g., Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 585 (1952).

### **Requested Relief**

Petitioners respectfully request that this Court grant the following relief:

- A. Issue a declaratory judgment that the Act violates the U.S. Constitution;
- B. Issue an order enjoining the Attorney General from enforcing the Act;
- C. Enter judgment in favor of Petitioners; and
- D. Grant any further relief that may be appropriate.

DATED: May 7, 2024

Andrew J. Pincus  
Avi M. Kupfer  
MAYER BROWN LLP  
1999 K Street, NW  
Washington, DC 20006  
Telephone: 202-263-3220  
Email:  
apincus@mayerbrown.com  
akupfer@mayerbrown.com

Respectfully submitted,

/s/ Alexander A. Berengaut  
Alexander A. Berengaut  
David M. Zions  
Megan A. Crowley  
COVINGTON & BURLING LLP  
One CityCenter  
850 Tenth Street, NW  
Washington, DC 20001  
Telephone: (202) 662-6000  
Email: aberengaut@cov.com  
dzions@cov.com  
mcrowley@cov.com

John E. Hall  
Anders Linderot  
COVINGTON & BURLING LLP  
The New York Times Building  
620 Eighth Avenue  
New York, New York 10018  
Telephone: (212) 841-1000  
Email: jhall@cov.com  
alinderot@cov.com

*Counsel for Petitioners*

**IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

<hr/>		)	
TIKTOK INC.,		)	
		)	
and		)	
		)	
BYTEDANCE LTD.,		)	
		)	
	<i>Petitioners,</i>	)	
		)	
v.		)	No. 24-1113
		)	
		)	
MERRICK B. GARLAND, in his official		)	
capacity as Attorney		)	
General of the United States,		)	
		)	
	<i>Respondent.</i>	)	
<hr/>		)	

**CORPORATE DISCLOSURE STATEMENT**

Petitioners state as follows:

ByteDance Ltd. is a privately held corporation incorporated in the Cayman Islands. ByteDance Ltd. subsidiaries provide a suite of more than a dozen products and services that allow people to connect with, create, and consume content on the Internet. ByteDance Ltd. has no

parent company, and no publicly traded company owns 10% or more of ByteDance Ltd.'s stock.

TikTok Inc. is a California-incorporated company that provides the TikTok platform in the United States. TikTok Inc. is a wholly owned subsidiary of TikTok LLC, which is a wholly owned subsidiary of TikTok Ltd. TikTok Ltd. is a wholly owned subsidiary of ByteDance Ltd. TikTok Inc. has no other parent company, and no publicly held corporation owns 10% or more of its stock.

/s/ Alexander A. Berengaut  
Alexander A. Berengaut

*Counsel for Petitioners*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 7th day of May, I caused copies of the foregoing Petition for Review and Corporate Disclosure Statement to be served upon the following recipients.

By certified mail, postage prepaid:

Merrick B. Garland  
Attorney General of the United States  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, DC 20530

By hand delivery:

Matthew M. Graves  
United States Attorney  
601 D Street, NW  
Washington, DC 20579

/s/ Alexander A. Berengaut  
Alexander A. Berengaut

*Counsel for Petitioners*

# EXHIBIT A

## H. R. 815—61

Fusion Development Strategy programs of the People's Republic of China, including the following:

- (1) A brief summary of each such identified field and its relevance to the military power and national security of the People's Republic of China.
- (2) The implications for the national security of the United States as a result of the leadership or dominance by the People's Republic of China in each such identified field and associated supply chains.
- (3) The identification of at least 10 entities domiciled in, controlled by, or directed by the People's Republic of China (including any subsidiaries of such entity), involved in each such identified field, and an assessment of, with respect to each such entity, the following:
  - (A) Whether the entity has procured components from any known United States suppliers.
  - (B) Whether any United States technology imported by the entity is controlled under United States regulations.
  - (C) Whether United States capital is invested in the entity, either through known direct investment or passive investment flows.
  - (D) Whether the entity has any connection to the People's Liberation Army, the Military-Civil Fusion program of the People's Republic of China, or any other state-sponsored initiatives of the People's Republic of China to support the development of national champions.
- (c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term “appropriate congressional committees” means—
  - (1) the Committee on Foreign Affairs of the House of Representatives;
  - (2) the Committee on Armed Services of the House of Representatives;
  - (3) the Committee on Foreign Relations of the Senate; and
  - (4) the Committee on Armed Services of the Senate.

## **DIVISION H—PROTECTING AMERICANS FROM FOREIGN ADVERSARY CONTROLLED APPLICATIONS ACT**

### **SEC. 1. SHORT TITLE.**

This division may be cited as the “Protecting Americans from Foreign Adversary Controlled Applications Act”.

### **SEC. 2. PROHIBITION OF FOREIGN ADVERSARY CONTROLLED APPLICATIONS.**

#### **(a) IN GENERAL.—**

(1) PROHIBITION OF FOREIGN ADVERSARY CONTROLLED APPLICATIONS.—It shall be unlawful for an entity to distribute, maintain, or update (or enable the distribution, maintenance, or updating of) a foreign adversary controlled application by carrying out, within the land or maritime borders of the United States, any of the following:



## H. R. 815—62

(A) Providing services to distribute, maintain, or update such foreign adversary controlled application (including any source code of such application) by means of a marketplace (including an online mobile application store) through which users within the land or maritime borders of the United States may access, maintain, or update such application.

(B) Providing internet hosting services to enable the distribution, maintenance, or updating of such foreign adversary controlled application for users within the land or maritime borders of the United States.

(2) APPLICABILITY.—Subject to paragraph (3), this subsection shall apply—

(A) in the case of an application that satisfies the definition of a foreign adversary controlled application pursuant to subsection (g)(3)(A), beginning on the date that is 270 days after the date of the enactment of this division; and

(B) in the case of an application that satisfies the definition of a foreign adversary controlled application pursuant to subsection (g)(3)(B), beginning on the date that is 270 days after the date of the relevant determination of the President under such subsection.

(3) EXTENSION.—With respect to a foreign adversary controlled application, the President may grant a 1-time extension of not more than 90 days with respect to the date on which this subsection would otherwise apply to such application pursuant to paragraph (2), if the President certifies to Congress that—

(A) a path to executing a qualified divestiture has been identified with respect to such application;

(B) evidence of significant progress toward executing such qualified divestiture has been produced with respect to such application; and

(C) there are in place the relevant binding legal agreements to enable execution of such qualified divestiture during the period of such extension.

(b) DATA AND INFORMATION PORTABILITY TO ALTERNATIVE APPLICATIONS.—Before the date on which a prohibition under subsection (a) applies to a foreign adversary controlled application, the entity that owns or controls such application shall provide, upon request by a user of such application within the land or maritime borders of United States, to such user all the available data related to the account of such user with respect to such application. Such data shall be provided in a machine readable format and shall include any data maintained by such application with respect to the account of such user, including content (including posts, photos, and videos) and all other account information.

(c) EXEMPTIONS.—

(1) EXEMPTIONS FOR QUALIFIED DIVESTITURES.—Subsection

(a)—

(A) does not apply to a foreign adversary controlled application with respect to which a qualified divestiture is executed before the date on which a prohibition under subsection (a) would begin to apply to such application; and

## H. R. 815—63

(B) shall cease to apply in the case of a foreign adversary controlled application with respect to which a qualified divestiture is executed after the date on which a prohibition under subsection (a) applies to such application.

(2) EXEMPTIONS FOR CERTAIN NECESSARY SERVICES.—Subsections (a) and (b) do not apply to services provided with respect to a foreign adversary controlled application that are necessary for an entity to attain compliance with such subsections.

(d) ENFORCEMENT.—

(1) CIVIL PENALTIES.—

(A) FOREIGN ADVERSARY CONTROLLED APPLICATION VIOLATIONS.—An entity that violates subsection (a) shall be subject to pay a civil penalty in an amount not to exceed the amount that results from multiplying \$5,000 by the number of users within the land or maritime borders of the United States determined to have accessed, maintained, or updated a foreign adversary controlled application as a result of such violation.

(B) DATA AND INFORMATION VIOLATIONS.—An entity that violates subsection (b) shall be subject to pay a civil penalty in an amount not to exceed the amount that results from multiplying \$500 by the number of users within the land or maritime borders of the United States affected by such violation.

(2) ACTIONS BY ATTORNEY GENERAL.—The Attorney General—

(A) shall conduct investigations related to potential violations of subsection (a) or (b), and, if such an investigation results in a determination that a violation has occurred, the Attorney General shall pursue enforcement under paragraph (1); and

(B) may bring an action in an appropriate district court of the United States for appropriate relief, including civil penalties under paragraph (1) or declaratory and injunctive relief.

(e) SEVERABILITY.—

(1) IN GENERAL.—If any provision of this section or the application of this section to any person or circumstance is held invalid, the invalidity shall not affect the other provisions or applications of this section that can be given effect without the invalid provision or application.

(2) SUBSEQUENT DETERMINATIONS.—If the application of any provision of this section is held invalid with respect to a foreign adversary controlled application that satisfies the definition of such term pursuant to subsection (g)(3)(A), such invalidity shall not affect or preclude the application of the same provision of this section to such foreign adversary controlled application by means of a subsequent determination pursuant to subsection (g)(3)(B).

(f) RULE OF CONSTRUCTION.—Nothing in this division may be construed—

(1) to authorize the Attorney General to pursue enforcement, under this section, other than enforcement of subsection (a) or (b);

## H. R. 815—64

(2) to authorize the Attorney General to pursue enforcement, under this section, against an individual user of a foreign adversary controlled application; or

(3) except as expressly provided herein, to alter or affect any other authority provided by or established under another provision of Federal law.

(g) DEFINITIONS.—In this section:

(1) CONTROLLED BY A FOREIGN ADVERSARY.—The term “controlled by a foreign adversary” means, with respect to a covered company or other entity, that such company or other entity is—

(A) a foreign person that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country;

(B) an entity with respect to which a foreign person or combination of foreign persons described in subparagraph (A) directly or indirectly own at least a 20 percent stake; or

(C) a person subject to the direction or control of a foreign person or entity described in subparagraph (A) or (B).

(2) COVERED COMPANY.—

(A) IN GENERAL.—The term “covered company” means an entity that operates, directly or indirectly (including through a parent company, subsidiary, or affiliate), a website, desktop application, mobile application, or augmented or immersive technology application that—

(i) permits a user to create an account or profile to generate, share, and view text, images, videos, real-time communications, or similar content;

(ii) has more than 1,000,000 monthly active users with respect to at least 2 of the 3 months preceding the date on which a relevant determination of the President is made pursuant to paragraph (3)(B);

(iii) enables 1 or more users to generate or distribute content that can be viewed by other users of the website, desktop application, mobile application, or augmented or immersive technology application; and

(iv) enables 1 or more users to view content generated by other users of the website, desktop application, mobile application, or augmented or immersive technology application.

(B) EXCLUSION.—The term “covered company” does not include an entity that operates a website, desktop application, mobile application, or augmented or immersive technology application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.

(3) FOREIGN ADVERSARY CONTROLLED APPLICATION.—The term “foreign adversary controlled application” means a website, desktop application, mobile application, or augmented or immersive technology application that is operated, directly or indirectly (including through a parent company, subsidiary, or affiliate), by—

(A) any of—

(i) ByteDance, Ltd.;

## H. R. 815—65

(ii) TikTok;

(iii) a subsidiary of or a successor to an entity identified in clause (i) or (ii) that is controlled by a foreign adversary; or

(iv) an entity owned or controlled, directly or indirectly, by an entity identified in clause (i), (ii), or (iii); or

(B) a covered company that—

(i) is controlled by a foreign adversary; and

(ii) that is determined by the President to present a significant threat to the national security of the United States following the issuance of—

(I) a public notice proposing such determination; and

(II) a public report to Congress, submitted not less than 30 days before such determination, describing the specific national security concern involved and containing a classified annex and a description of what assets would need to be divested to execute a qualified divestiture.

(4) FOREIGN ADVERSARY COUNTRY.—The term “foreign adversary country” means a country specified in section 4872(d)(2) of title 10, United States Code.

(5) INTERNET HOSTING SERVICE.—The term “internet hosting service” means a service through which storage and computing resources are provided to an individual or organization for the accommodation and maintenance of 1 or more websites or online services, and which may include file hosting, domain name server hosting, cloud hosting, and virtual private server hosting.

(6) QUALIFIED DIVESTITURE.—The term “qualified divestiture” means a divestiture or similar transaction that—

(A) the President determines, through an interagency process, would result in the relevant foreign adversary controlled application no longer being controlled by a foreign adversary; and

(B) the President determines, through an interagency process, precludes the establishment or maintenance of any operational relationship between the United States operations of the relevant foreign adversary controlled application and any formerly affiliated entities that are controlled by a foreign adversary, including any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing.

(7) SOURCE CODE.—The term “source code” means the combination of text and other characters comprising the content, both viewable and nonviewable, of a software application, including any publishing language, programming language, protocol, or functional content, as well as any successor languages or protocols.

(8) UNITED STATES.—The term “United States” includes the territories of the United States.

**SEC. 3. JUDICIAL REVIEW.**

(a) RIGHT OF ACTION.—A petition for review challenging this division or any action, finding, or determination under this division

H. R. 815—66

may be filed only in the United States Court of Appeals for the District of Columbia Circuit.

(b) **EXCLUSIVE JURISDICTION.**—The United States Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over any challenge to this division or any action, finding, or determination under this division.

(c) **STATUTE OF LIMITATIONS.**—A challenge may only be brought—

(1) in the case of a challenge to this division, not later than 165 days after the date of the enactment of this division; and

(2) in the case of a challenge to any action, finding, or determination under this division, not later than 90 days after the date of such action, finding, or determination.

## **DIVISION I—PROTECTING AMERICANS’ DATA FROM FOREIGN ADVERSARIES ACT OF 2024**

### **SEC. 1. SHORT TITLE.**

This division may be cited as the “Protecting Americans’ Data from Foreign Adversaries Act of 2024”.

### **SEC. 2. PROHIBITION ON TRANSFER OF PERSONALLY IDENTIFIABLE SENSITIVE DATA OF UNITED STATES INDIVIDUALS TO FOREIGN ADVERSARIES.**

(a) **PROHIBITION.**—It shall be unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to—

(1) any foreign adversary country; or

(2) any entity that is controlled by a foreign adversary.

(b) **ENFORCEMENT BY FEDERAL TRADE COMMISSION.**—

(1) **UNFAIR OR DECEPTIVE ACTS OR PRACTICES.**—A violation of this section shall be treated as a violation of a rule defining an unfair or a deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) **POWERS OF COMMISSION.**—

(A) **IN GENERAL.**—The Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section.

(B) **PRIVILEGES AND IMMUNITIES.**—Any person who violates this section shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(3) **AUTHORITY PRESERVED.**—Nothing in this section may be construed to limit the authority of the Commission under any other provision of law.

(c) **DEFINITIONS.**—In this section:

(1) **COMMISSION.**—The term “Commission” means the Federal Trade Commission.