

Nos. 24-656 and 24-657

---

IN THE

**Supreme Court of the United States**

---

TIKTOK INC. AND BYTEDANCE LTD.,

*Petitioners,*

v.

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

*Respondent.*

---

BRIAN FIREBAUGH ET AL.,

*Petitioners,*

v.

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

*Respondent.*

---

**On Writs Of Certiorari  
To The United States Court Of Appeals  
For The D.C. Circuit**

---

**JOINT APPENDIX**

**Volume I of II (Pages 1–516)**

---

ELIZABETH B. PRELOGAR

*Counsel of Record  
for Respondent*

Solicitor General

DEPARTMENT OF JUSTICE

950 Pennsylvania Ave., NW

Washington, DC 20530

(202) 514-2217

supremectbriefs@usdoj.gov

NOEL J. FRANCISCO

*Counsel of Record  
for Petitioners*

*TikTok Inc. and*

*ByteDance Ltd.*

JONES DAY

51 Louisiana Ave., NW

Washington, DC 20001

(202) 879-3939

njfrancisco@jonesday.com

JEFFREY L. FISHER

*Counsel of Record*

*for Creator Petitioners*

O'MELVENY & MYERS LLP

2765 Sand Hill Road

Menlo Park, CA 94025

(650) 473-2600

jlfisher@omm.com

---

PETITIONS FOR CERTIORARI FILED: DECEMBER 16, 2024

CERTIORARI GRANTED: DECEMBER 18, 2024

## Table of Contents

### Volume I

Opinion of the United States Court of Appeals for the District of Columbia Circuit (Dec. 6, 2024).....	JA 1
Judgment of the United States Court of Appeals for the District of Columbia Circuit (Dec. 6, 2024).....	JA 93
TikTok Petitioners’ Petition for Review .....	JA 94
Creator Petitioners’ Petition for Review.....	JA 161
BASED Politics Inc.’s Petition for Review.....	JA 193
H.R. Comm. on Energy & Com., <i>Protecting Americans from Foreign Adversary Controlled Applications Act</i> , H.R. Rep. No. 118-417 (2024) .....	JA 210
170 Cong. Rec. S2629 (daily ed. Apr. 8, 2024) (excerpts) .....	JA 228
170 Cong. Rec. S2943 (daily ed. Apr. 23, 2024) (excerpts) .....	JA 231
Draft National Security Agreement (Aug. 23, 2022) (redacted) .....	JA 236
Nicholas Kaufman et al., U.S.-China Econ. & Sec. Rev. Comm’n, <i>Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes</i> (Apr. 14, 2023).....	JA 339

Sen. Tom Cotton (@SenTomCotton), X (Mar. 10, 2024) .....JA 348

Sapna Maheshawri et al., *House Passes Bill to Force TikTok Sale from Chinese Owner or Ban the App*, N.Y. Times (Mar. 13, 2024).....JA 349

Transcript of Interview with Sen. Mark Warner, Fox News (Mar. 14, 2024) (excerpts).....JA 356

Transcript of Keynote Conversation Between Secretary of State Antony Blinken and Sen. Mitt Romney, McCain Institute (May 3, 2024) (excerpts) .....JA 363

Declaration of Randal S. Milch .....JA 367

Declaration of Christopher P. Simkins.....JA 412

Declaration of Steven Weber.....JA 451

Declaration of Adam Presser .....JA 481

**Volume II**

Declaration of Talia Cadet .....JA 517

Declaration of Brian Firebaugh.....JA 527

Declaration of Steven King .....JA 537

Declaration of Timothy Martin.....JA 544

Declaration of Chloe Joy Sexton.....JA 553

Declaration of Kiera Spann.....JA 561

Declaration of Christopher Townsend.....	JA 572
Declaration of Paul Tran.....	JA 582
<i>How TikTok recommends videos #ForYou</i> , TikTok (June 18, 2020) .....	JA 590
<i>How TikTok recommends content</i> , TikTok .....	JA 595
Alexandra Garfinkle, <i>TikTok: Are influencers panicking about bans? We asked three to weigh in.</i> , Yahoo! Finance (Jan. 19, 2023).....	JA 601
Steven Lee Myers et al., <i>The Consequences of Elon Musk’s Ownership of X</i> , N.Y. Times (Oct. 27, 2023) .....	JA 607
Declaration of Brad Polumbo.....	JA 616
Declaration of Hannah Cox.....	JA 619
Declaration of Casey Blackburn (redacted).....	JA 625
Declaration of Kevin Vorndran (redacted) .....	JA 655
Declaration of David Newman (redacted) .....	JA 668
Reply Declaration of Christopher P. Simkins .....	JA 714
Reply Declaration of Steven Weber .....	JA 747
Declaration of William C. Farrell .....	JA 769
Transcript of Mar. 7, 2024 House Energy & Com. Comm. Hr’g (redacted; excerpts).....	JA 781

Declaration of Blake Chandlee .....	JA 801
Supplemental Declaration of Talia Cadet .....	JA 812
Supplemental Declaration of Brian Firebaugh.....	JA 816
Supplemental Declaration of Steven King .....	JA 821
Supplemental Declaration of Timothy Martin .....	JA 825
Supplemental Declaration of Chloe Joy Sexton.....	JA 829
Supplemental Declaration of Kiera Spann.....	JA 832
Supplemental Declaration of Christopher Townsend .....	JA 837
Supplemental Declaration of Paul Tran.....	JA 842
Supplemental Declaration of Hannah Cox.....	JA 846

**United States Court of Appeals**  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

Argued September 16, 2024

Decided December 6, 2024

No. 24-1113

TIKTOK INC. AND BYTEDANCE LTD.,  
PETITIONERS

v.

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

---

Consolidated with 24-1130, 24-1183

---

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

---

*Andrew J. Pincus* argued the cause for TikTok Petitioners.  
With him on the briefs were *Avi M. Kupfer*, *Alexander A.  
Berengaut*, *David M. Zions*, *Megan A. Crowley*, and *John E.  
Hall*.

*Jeffrey L. Fisher* argued the cause for Creator Petitioners.  
With him on the briefs were *Ambika Kumar*, *Tim Cunningham*,

*Xiang Li, Elizabeth A. McNamara, Chelsea T. Kelly, James R. Sigel, Adam S. Sieff, and Joshua Revesz.*

*Jacob Huebert and Jeffrey M. Schwab* were on the briefs for petitioner BASED Politics, Inc.

*David Greene* was on the brief for *amici curiae* Electronic Frontier Foundation, et al. in support of petitioners.

*Jameel Jaffer and Eric Columbus* were on the brief for *amici curiae* the Knight First Amendment Institute at Columbia University, et al. in support of petitioners.

*Edward Andrew Paltzik and Serge Krimmus* were on the brief for *amicus curiae* HungryPanda US, Inc. in support of petitioners.

*Matt K. Nguyen, Travis LeBlanc, Robert H. Denniston, Kathleen R. Hartnett, and Jamie D. Robertson* were on the brief for *amici curiae* Social and Racial Justice Community Nonprofits in support of petitioners.

*Nicholas Reddick and Meryl Conant Governski* were on the brief for *amici curiae* First Amendment Law Professors in support of petitioners.

*Thomas A. Berry* was on the brief for *amicus curiae* the Cato Institute in support of petitioners.

*Mark Davies, Ethan L. Plail, and Edred Richardson* were on the brief for *amici curiae* Professors Mueller, Edgar, Aaronson, and Klein in support of petitioners.

*Aaron D. Van Oort* was on the brief for *amicus curiae* Professor Matthew Steilen in support of petitioners.

*Daniel Tenny*, Attorney, U.S. Department of Justice, argued the cause for respondent. With him on the brief were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, *Brian D. Netter*, Deputy Assistant Attorney General, *Mark R. Freeman*, *Sharon Swingle*, *Casen B. Ross*, *Sean R. Janda*, and *Brian J. Springer*, Attorneys, *Matthew G. Olsen*, Assistant Attorney General for National Security, *Tyler J. Wood*, Deputy Chief, Foreign Investment Review Section, and *Tricia Wellman*, Acting General Counsel, Office of the Director of National Intelligence.

*Thomas R. McCarthy* was on the brief for *amici curiae* Former National Security Officials in support of respondent.

*Joel L. Thayer* was on the brief for *amici curiae* Campaign for Uyghurs, et al. in support of respondent.

*Joel L. Thayer* was on the brief for *amici curiae* Zephyr Teachout, et al. in support of respondent.

*Thomas M. Johnson, Jr.*, *Jeremy J. Broggi*, and *Joel S. Nolette* were on the brief for *amici curiae* Chairman of the Select Committee on the CCP *John R. Moolenaar*, et al. in support of respondent.

*David H. Thompson*, *Brian W. Barnes*, and *Megan M. Wold* were on the brief for *amicus curiae* Professor *D. Adam Candeub* in support of respondent.

*Thomas M. Johnson, Jr.*, *Jeremy J. Broggi*, and *Michael J. Showalter* were on the brief for *amici curiae* Former Chairman of the Federal Communications Commission *Ajit V. Pai* and Former Assistant Secretary of the Treasury for Investment Security *Thomas P. Feddo* in support of respondent.



*Jonathan Berry, Michael Buschbacher, Jared M. Kelson, James R. Conde, and William P. Barr* were on the brief for *amicus curiae* American Free Enterprise Chamber of Commerce in support of respondent.

*Austin Knudsen*, Attorney General, Office of the Attorney General for the State of Montana, *Christian B. Corrigan*, Solicitor General, *Peter M. Torstensen, Jr.*, Deputy Solicitor General, *Jason S. Miyares*, Attorney General, Office of the Attorney General for the Commonwealth of Virginia, *Erika L. Maley*, Solicitor General, *Kevin M. Gallagher*, Principal Deputy Solicitor General, *Steve Marshall*, Attorney General, Office of the Attorney General for the State of Alabama, *Treg Taylor*, Attorney General, Office of the Attorney General for the State of Alaska, *Tim Griffin*, Attorney General, Office of the Attorney General for the State of Arkansas, *Ashley Moody*, Attorney General, Office of the Attorney General for the State of Florida, *Christopher M. Carr*, Attorney General, Office of the Attorney General for the State of Georgia, *Raúl R. Labrador*, Attorney General, Office of the Attorney General for the State of Idaho, *Theodore E. Rokita*, Attorney General, Office of the Attorney General for the State of Indiana, *Brenna Bird*, Attorney General, Office of the Attorney General for the State of Iowa, *Russell Coleman*, Attorney General, Office of the Attorney General for the Commonwealth of Kentucky, *Liz Murrill*, Attorney General, Office of the Attorney General for the State of Louisiana, *Lynn Fitch*, Attorney General, Office of the Attorney General for the State of Mississippi, *Andrew Bailey*, Attorney General, Office of the Attorney General for the State of Missouri, *Michael T. Hilgers*, Attorney General, Office of the Attorney General for the State of Nebraska, *John M. Formella*, Attorney General, Office of the Attorney General for the State of New Hampshire, *Gentner F. Drummond*, Attorney General, Office of the Attorney General for the State of Oklahoma, *Alan Wilson*, Attorney General, Office of the

Attorney General for the State of South Carolina, *Marty J. Jackley*, Attorney General, Office of the Attorney General for the State of South Dakota, *Jonathan Skrmetti*, Attorney General, Office of the Attorney General for the State of Tennessee, and *Sean D. Reyes*, Attorney General, Office of the Attorney General for the State of Utah, were on the brief for *amici curiae* State of Montana, Virginia, and 19 Other States in support of respondent.

*Peter C. Choharis* and *Arnon D. Siegel* were on the brief for *amicus curiae* the Foundation for Defense of Democracies in support of respondent.

Before: SRINIVASAN, *Chief Judge*, RAO, *Circuit Judge*, and GINSBURG, *Senior Circuit Judge*.

Opinion for the Court filed by *Senior Circuit Judge* GINSBURG.

Opinion concurring in part and concurring in the judgment filed by *Chief Judge* SRINIVASAN.

I. Background	8
A. The TikTok Platform	8
B. The Petitioners	9
C. National Security Concerns	11
D. The Act	15
1. Foreign adversary controlled applications	16
2. Prohibitions	18
3. The divestiture exemption	19
E. Procedural History	20
II. Analysis	20
A. Standing and Ripeness	21
B. The First Amendment	24
1. Heightened scrutiny applies.	24
2. The Act satisfies strict scrutiny.	32
a. The Government's justifications are compelling.	33
(i) National security justifications	33
(ii) Data collection	38
(iii) Content manipulation	42
b. The Act is narrowly tailored.	48
(i) TikTok's proposed NSA	49
(ii) Other options	53
(iii) Overinclusive / underinclusive	55
C. Equal Protection	57
D. The Bill of Attainder Clause	59
E. The Takings Clause	63
F. Alternative Relief	64
III. Conclusion	65

GINSBURG, *Senior Circuit Judge*: On April 24, 2024 the President signed the Protecting Americans from Foreign Adversary Controlled Applications Act into law. Pub. L. No. 118-50, div. H. The Act identifies the People’s Republic of China (PRC) and three other countries as foreign adversaries of the United States and prohibits the distribution or maintenance of “foreign adversary controlled applications.”<sup>1</sup> Its prohibitions will take effect on January 19, 2025 with respect to the TikTok platform.

Three petitions — filed by ByteDance Ltd. and TikTok, Inc.; Based Politics, Inc.; and a group of individuals (“Creators”) who use the TikTok platform — which we have consolidated, all present constitutional challenges to the Act. We conclude the portions of the Act the petitioners have standing to challenge, that is the provisions concerning TikTok and its related entities, survive constitutional scrutiny. We therefore deny the petitions.

---

<sup>1</sup> A foreign adversary controlled application is defined in § 2(g)(3) as “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.; (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 [certain procedures].

## I. Background

This court has original and exclusive jurisdiction over this case pursuant to Section 3 of the Act. The parties have submitted several evidentiary appendices in support of their positions, including sworn declarations from various experts. In reviewing this material, we consider whether there is a genuine dispute as to any material fact. *Cf.* Fed. R. Civ. P. 56(a), (c)(4). Here, no dispute of “essential facts” stands in the way of our deciding this case on the merits of the parties’ legal arguments. *See Cal. ex rel. State Lands Comm’n v. United States*, 457 U.S. 273, 278 (1982); *South Carolina v. Katzenbach*, 383 U.S. 301, 307 (1966).

### A. The TikTok Platform

TikTok is a social-media platform that lets users create, upload, and watch short video clips overlaid with text, voiceovers, and music. For each individual viewer, the platform creates a continuous sequence of videos based upon that user’s behavior and several other factors, with the aim of keeping that user engaged. The TikTok platform has approximately 170 million monthly users in the United States and more than one billion users worldwide.

What a TikTok user sees on the platform is determined by a recommendation engine, company content moderation decisions, and video promotion and filtering decisions. The recommendation engine is an algorithm that displays videos based upon content metadata and user behavior. It identifies a pool of candidate videos for a user, then scores and ranks those videos using machine-learning models designed to determine which video(s) would be most appealing to the user. The source code for the engine was originally developed by ByteDance, a company based in China that is the ultimate parent of TikTok. According to TikTok, the global TikTok team, which includes

Chinese engineers, “continually develop[s]” the recommendation engine and platform source code. As we explain in more detail below, the recommendation engine for the version of the platform that operates in the United States is deployed to a cloud environment run by Oracle Corporation.

Content moderation decisions involve a combination of machine and human actions. According to TikTok every video on the TikTok platform goes through “automated moderation” and if deemed potentially problematic is sent to a human moderator for review. TikTok’s Head of Operations and Trust & Safety approves the “community guidelines” that drive content moderation on the platform.

Video promotion (also called “heating”) and demotion (also called “filtering”) decisions are used to advance TikTok’s commercial or other goals. These decisions involve promoting or limiting specific videos on the platform. According to TikTok, each video that is promoted is first reviewed by a human. Review teams are regionalized so that videos promoted in the United States are reviewed by U.S.-based reviewers. With respect to filtering, the platform follows “a set of rules to filter out and disperse certain content.”

## **B. The Petitioners**

Three groups of petitioners challenge the Act on constitutional grounds: ByteDance Ltd. and TikTok, Inc.; Based Politics, Inc.; and the self-styled Creators, eight individuals who use the TikTok platform. We refer to the latter two groups collectively as the User Petitioners. Where the corporate structure of ByteDance affects our analysis, we identify the relevant corporate entity by name. Otherwise, we refer generally to the constellation of ByteDance entities as TikTok. Because PRC control of the TikTok platform is central to this case, we

provide the following overview of the relevant corporate relationships.

ByteDance Ltd., the ultimate parent company of TikTok, is incorporated in the Cayman Islands. The Government characterizes ByteDance as headquartered in China and ByteDance acknowledges that it has significant operations there.<sup>2</sup> ByteDance provides more than a dozen products through various operating subsidiaries, including Douyin, which is the counterpart to TikTok in China. The company was founded by Yiming Zhang, a Chinese national. Zhang retains 21 percent ownership of the company.

TikTok Ltd. is a wholly owned subsidiary of ByteDance and is also incorporated abroad. TikTok Ltd. operates the TikTok platform globally, except in China. The Government refers to TikTok entities that operate the platform outside the United States as “TikTok Global” and its U.S. operations as “TikTok US.”

TikTok Ltd. wholly owns TikTok LLC, which in turn wholly owns TikTok, Inc., a California corporation that provides the TikTok platform to users in the United States. According to a TikTok declarant, TikTok’s “U.S. application and global application are highly integrated,” and the “global TikTok application itself is highly integrated with ByteDance.” Because the TikTok “platform and the content [are] global, the teams working on the platform, and the tools they use, necessarily must be, as well.” According to TikTok, one of ByteDance’s roles is “development of portions of the computer code that runs the TikTok platform.” In the Government’s view, TikTok “would try to comply if the PRC asked for specific actions to be taken to manipulate content for

---

<sup>2</sup> We use “China” when referring to the country and PRC when referencing its government.

ensorship, propaganda, or other malign purposes on TikTok US.”

TikTok U.S. Data Security Inc. (TTUSDS) is a wholly owned subsidiary of TikTok, Inc., incorporated in Delaware. TikTok created TTUSDS to limit ByteDance’s access to the data of TikTok’s users in the United States and to monitor the security of the platform. TikTok represents that TTUSDS employees are separated from other TikTok employees, and that it partnered with Oracle to migrate the U.S. version of the TikTok platform into a cloud environment run by Oracle. TikTok also represents that TTUSDS and Oracle review updates to the platform made by ByteDance’s non-TTUSDS employees, and that Oracle has full access to TikTok’s source code. According to TikTok, TTUSDS is also responsible for deploying the recommendation engine in the United States, and TTUSDS signs off on any decision to promote or demote content in the United States.

### **C. National Security Concerns**

As relevant here, the Executive<sup>3</sup> first became concerned about the PRC’s influence over TikTok in 2018 when ByteDance relaunched the platform in the United States following its acquisition of Musical.ly. In 2019, upon finding that “foreign adversaries” were “exploiting vulnerabilities in information and communications technology and services,” President Trump declared a national emergency. *Securing the Information and Communications Technology and Services Supply Chain*, Exec. Order No. 13873, 84 Fed. Reg. 22689, 22689 (May 15, 2019). Later that year, the Committee on Foreign Investment in the United States (CFIUS), which comprises the heads of several Executive Branch agencies, sent

---

<sup>3</sup> The Executive refers variously to the President, Executive Branch agencies, including the intelligence agencies, and officials thereof.



a questionnaire to ByteDance about national security concerns related to ByteDance's acquisition of Musical.ly. This began a lengthy investigatory process that culminated on August 1, 2020 with CFIUS concluding that TikTok could not sufficiently mitigate its national security concerns and referring the transaction to the President. The President, acting on that referral, ordered ByteDance to divest any "assets or property" that "enable or support ByteDance's operation of the TikTok application in the United States." *Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297, 51297 (Aug. 14, 2020).

President Trump separately invoked his powers under the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act to address "the threat posed by one mobile application in particular, TikTok." *Addressing the Threat Posed by TikTok*, Exec. Order No. 13942, 85 Fed. Reg. 48637, 48637 (Aug. 6, 2020). President Trump prohibited certain "transactions" with ByteDance or its subsidiaries, *id.* at 48638, and the Secretary of Commerce later published a list of prohibited transactions, 85 Fed. Reg. 60061 (Sept. 24, 2020). Litigation ensued, and two courts enjoined the President's prohibitions under the IEEPA as exceeding his authority under that law. *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 102 (D.D.C. 2020); *Maryland v. Trump*, 498 F. Supp. 3d 624, 638, 641–45 (E.D. Pa. 2020).

In 2021, President Biden withdrew President Trump's IEEPA executive order and issued a new one. In the new order, the President identified the PRC as "a foreign adversary" that "continues to threaten the national security, foreign policy, and economy of the United States" through its control of "software applications" used in the United States. *Protecting Americans' Sensitive Data From Foreign Adversaries*, Exec. Order No. 14034, 86 Fed. Reg. 31423, 31423 (June 9, 2021). President

Biden elaborated that “software applications” can provide foreign adversaries with “vast swaths of information from users,” and that the PRC’s “access to large repositories” of such data “presents a significant risk.” *Id.* President Biden directed several executive agencies to provide risk mitigation options, and he asked for recommended “executive and legislative actions” to counter risks “associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.” *Id.* The following year, President Biden signed into law a bill prohibiting the use of TikTok on government devices. *See generally* Pub. L. No. 117-328, div. R, 136 Stat. 5258 (2022).

Litigation regarding President Trump’s divestiture order pursuant to CFIUS’s referral began when TikTok filed suit in this court challenging the constitutionality of the order. *See* Pet. for Review, *TikTok Inc. v. CFIUS*, No. 20-1444 (2020). At the request of the parties, in February 2021 this court placed that case in abeyance while the new administration considered the matter and the parties negotiated over an alternative remedy that would sufficiently address the Executive’s national security concerns.

During 2021 and 2022, TikTok submitted multiple drafts of its proposed National Security Agreement (NSA) and Executive Branch officials held numerous meetings to consider TikTok’s submissions. According to TikTok, there were “at least” 14 meetings or calls, nine written presentations by TikTok, and 15 email exchanges in which “CFIUS posed questions related to [TikTok’s] operations and the NSA terms.” A TikTok declarant describes the negotiations as “protracted, detailed, and productive,” and the Government similarly characterizes them as “significant” and “intensive.” Also as part of the process, “Executive Branch negotiators engaged in

extensive, in-depth discussions with Oracle, the proposed Trusted Technology Provider, whose responsibility under the proposed mitigation structure included storing data in the United States, performing source code review, and ensuring safety of the operation of the TikTok platform in the United States.”

In August 2022, TikTok submitted its last proposal. Although the parties dispute certain details about how to interpret specific provisions, the broad contours of TikTok’s proposed NSA are undisputed. Three aspects of the proposal bear emphasis.

First, the proposal purported to give TikTok operational independence from ByteDance by creating a new entity insulated from the influence of ByteDance, namely TTUSDS. The key management personnel of TTUSDS were to be subject to approval by the Government.

Second, the proposed NSA would create three tiers of data to limit the ability of ByteDance to access the data of TikTok’s users in the United States. Protected Data generally would encompass personal information about TikTok’s U.S. users — such as their usernames, passwords, user-created content, and any other personally identifiable information — unless such data were classified as Excepted Data or Public Data. Sharing of Protected Data with ByteDance would be prohibited except pursuant to limited-access protocols. Excepted Data would include data that platform users authorized to be shared with TikTok or its affiliates; certain defined data fields; and encrypted usernames, phone numbers, email addresses, etc., for routing to the United States. Public Data would include data generally accessible to platform users, as well as any content a user decides to make public. Under the proposed NSA, TikTok could send Excepted Data and Public Data to ByteDance.

Third, the proposal provided for a “trusted third party,” Oracle, to inspect the source code, including TikTok’s recommendation engine. It also gave the Government authority, under certain circumstances, to instruct TikTok to shut down the platform in the United States, which TikTok calls a “kill switch.”

The Executive determined the proposed NSA was insufficient for several reasons. Most fundamentally, certain data of U.S. users would still flow to China and ByteDance would still be able to exert control over TikTok’s operations in the United States. The Executive also did not trust that ByteDance and TTUSDS would comply in good faith with the NSA. Nor did the Executive have “sufficient visibility [into] and resources to monitor” compliance. In the Executive’s view, divestment was the only solution that would adequately address its national security concerns. TikTok nevertheless voluntarily implemented some of its proposed mitigation measures.

#### **D. The Act**

In the months leading to passage of the Act, the Congress conducted a series of classified briefings and hearings regarding the Government’s national security concerns. The Congress then debated and passed the Act as one part of a broader appropriations bill, which also included the Protecting Americans’ Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50, div. I (2024), hereinafter the Data Broker Law. The Act and the Data Broker Law include nearly identical definitions of “foreign adversary country” and “controlled by a foreign adversary.” Their aims also overlap. Section 2(a) of the Data Broker Law prohibits third party data brokers from transferring “personally identifiable sensitive data of a United States individual” to a foreign adversary country or an entity “controlled by a foreign adversary.” The Act complements that

provision by limiting the ability of foreign adversaries to collect data directly through adversary controlled applications.

The Act itself is narrowly constructed to counter foreign adversary control through divestiture. Three aspects of the Act are particularly relevant to this case: (1) the definition of foreign adversary controlled applications, (2) prohibitions in the Act, and (3) the divestiture option.

### **1. Foreign adversary controlled applications**

The Act defines a Foreign Adversary Controlled Application as “a website, desktop application, mobile application, or augmented or immersive technology application that is operated, directly or indirectly” by either of two distinct groups. § 2(g)(3). The first group consists of the ByteDance constellation of entities, including TikTok, which is identified by name. § 2(g)(3)(A). The second group consists of every covered company<sup>4</sup> that is determined by the President to present a

---

<sup>4</sup> The term “covered company” is defined as “an entity that operates . . . 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

significant threat to national security. Specifically, it includes any “covered company” that:

- (i) is controlled by a foreign adversary;<sup>5</sup> 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

---

application, or augmented or immersive technology application.

§ 2(g)(2)(A). The term excludes, however, entities that operate an “application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.”  
§ 2(g)(2)(B).

<sup>5</sup> The term “controlled by a foreign adversary” means a “covered company or other entity” that 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(g)(1). The definition of “foreign adversary country” encompasses China, Russia, Iran, and North Korea. § 2(g)(2) (defining the term by reference to 10 U.S.C. § 4872(d)(2)).

what assets would need to be divested to execute a qualified divestiture.

§ 2(g)(3)(B).

## **2. Prohibitions**

The Act contains prohibitions, § 2(a), and a “data and information portability” requirement, § 2(b). The prohibitions do not directly proscribe conduct by an entity that owns a foreign adversary controlled application. Instead, they bar others from providing critical support in the United States for such an application. Specifically, the Act makes it “unlawful for an entity to distribute, maintain, or update” a foreign adversary controlled application in any of two ways:

- (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(a)(1).

With respect to TikTok, the prohibitions take effect 270 days after the Act was passed into law, that is, on January 19, 2025. § 2(a)(2)(A). With respect to applications subject to the generally applicable provisions, the prohibitions take effect 270 days after “the relevant determination of the President.”

§ 2(a)(2)(B). In both situations, the President can grant a one-time, 90-day extension under specific circumstances not relevant here. § 2(a)(3).

Failure to comply with the Act can result in substantial monetary penalties. § 2(d)(1). To enforce the Act the Attorney General, following an investigation, can file suit in an appropriate district court. § 2(d)(2).

### **3. The divestiture exemption**

Section 2(c) of the Act provides an exemption “for qualified divestitures.” That is, the prohibitions do not apply if “a qualified divestiture is executed before the date on which a prohibition under subsection (a) would begin to apply.” § 2(c)(1)(A). If a qualified divestiture is executed after that date, then the prohibitions “shall cease to apply.” § 2(c)(1)(B). A “qualified divestiture” is defined as a 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.

§ 2(g)(6).



### **E. Procedural History**

This case concerns three petitions challenging the Act that this court consolidated for review. On May 17, 2024 the parties jointly asked this Court to expedite the case. The parties advised that they intended to append evidentiary materials to their briefs. The Government noted that it was evaluating the need to file an ex parte evidentiary submission given the classified material implicated by the case. The petitioners reserved the right to object to any such submission.

The parties ultimately submitted evidence with their briefs. TikTok's submission included several expert declarations as well as a declaration from its Head of Operations and Trust & Safety. The User Petitioners filed declarations underscoring the diverse ways in which they use the TikTok platform. The Government filed declarations explaining its national security concerns and why it found TikTok's proposed NSA insufficient to meet those concerns. TikTok filed rebuttal declarations with its reply brief.

Portions of the Government's brief and evidentiary submission were redacted because they contain classified information. The Government filed a motion requesting leave to file unredacted versions of its brief and supporting evidence under seal and ex parte, which documents the Government later lodged with this court. The petitioners opposed the Government's motion and alternatively moved this court to appoint a special master and issue a temporary injunction in order to mitigate prejudice arising from the Government's classified filings.

### **II. Analysis**

The petitioners seek a declaratory judgment that the Act violates the Constitution and an order enjoining the Attorney

General from enforcing it. Because the petitioners are bringing a pre-enforcement challenge to the Act, we must determine the extent to which this court can consider their claims consistent with the standing aspect of the “case or controversy” requirement of Article III of the Constitution. We conclude that TikTok has standing to challenge those portions of the Act that directly affect the activities of ByteDance and its affiliates. We further conclude that TikTok’s challenge to those portions of the Act is ripe.

On the merits, we reject each of the petitioners’ constitutional claims. As we shall explain, the parts of the Act that are properly before this court do not contravene the First Amendment to the Constitution of the United States, nor do they violate the Fifth Amendment guarantee of equal protection of the laws; constitute an unlawful bill of attainder, in violation of Article I, § 9, clause 3; or work an uncompensated taking of private property in violation of the Fifth Amendment.

#### **A. Standing and Ripeness**

We have an independent duty to assure ourselves that the petitioners and their claims satisfy the requirements of Article III. *Exelon Corp. v. FERC*, 911 F.3d 1236, 1240 (D.C. Cir. 2018). TikTok’s claims all relate to how the Act applies to the TikTok platform; it has not, for example, meaningfully developed claims regarding other services provided by other ByteDance subsidiaries. Nor does it claim the generally applicable portions of the Act are unconstitutional as applied to other companies. TikTok instead seeks to enjoin the enforcement of the prohibitions on hosting the TikTok platform, which TikTok contends are unconstitutional irrespective of whether they are imposed based upon the generally applicable framework or upon the TikTok-specific provisions of the Act. At the same time, the User Petitioners claim the Act in its entirety is

“facially invalid under the First Amendment,” which need not detain us.<sup>6</sup> Creator Reply Br. 30–31.

“To establish standing for a pre-enforcement challenge, a plaintiff must demonstrate first an intention to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute and, second, that there exists a credible threat of prosecution thereunder.” *Muthana v. Pompeo*, 985 F.3d 893, 911 (D.C. Cir. 2021) (cleaned up). This inquiry is slightly more refined in cases that involve the potential future regulation of third parties. To establish standing in such circumstances, a plaintiff must demonstrate it is “likely that the government’s regulation . . . of someone else will cause a concrete and particularized injury in fact to the unregulated plaintiff.” *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 385 n.2 (2024).

Ripeness is “related” but focuses “on the timing of the action rather than on the parties seeking to bring it.” *Navegar, Inc. v. United States*, 103 F.3d 994, 998 (D.C. Cir. 1997). Courts consider (1) hardship to the parties and (2) fitness for judicial resolution when assessing ripeness. *Id.* The purposes of the ripeness doctrine are to avoid abstract argument, promote judicial economy, and ensure an adequate record. *Id.*

TikTok and its claims challenging enforcement of the prohibitions of the Act based upon the TikTok-specific provisions clearly satisfy the requirements respectively for standing and ripeness. The prohibitions based upon those provisions

---

<sup>6</sup> The User Petitioners have not demonstrated that “a substantial number of” the Act’s “applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2397 (2024) (cleaned up). Indeed, the core of the Act — its application as to TikTok — is valid for the reasons we explain in this opinion.

take effect by operation of law on January 19, 2025. After that date, third parties that make the TikTok platform available in the United States would run a significant risk of incurring monetary penalties under § 2(d)(1). Even if the Act went unenforced, the risk of penalties alone could cause third parties to suspend support for the TikTok platform, such as by removing it from online marketplaces, and an injunction would prevent that harm. TikTok therefore has Article III standing to pursue its claims.

The ripeness inquiry is likewise straightforward. TikTok risks severe hardship from delayed review, and we have an adequate record on which to resolve the company's challenges to the constitutionality of the TikTok-specific provisions of the Act.

To the extent TikTok seeks to enjoin future enforcement of the prohibitions under the generally applicable track, TikTok does not have standing. Nor if it did would such a request be ripe for judicial review. Recall that applying the prohibitions under the generally applicable framework requires certain procedural steps and a presidential determination pursuant to § 2(g)(3)(B). Those steps include public notice, a description of the national security concern, a classified annex, and a description of assets to be divested. § 2(g)(3)(B)(ii). The President has not invoked those procedures with respect to TikTok (or any other company), and it would be self-evidently premature for the court even to consider a request for an injunction against the President ever doing so. We consequently limit our analysis to the constitutionality of the Act as applied to the TikTok-specific provisions that will go into effect next month.<sup>7</sup>

---

<sup>7</sup> Having concluded that TikTok has standing, we need not separately analyze whether the User Petitioners have standing to raise the same claims. *See Carpenters Indus. Council v. Zinke*, 854 F.3d 1, 9 (D.C. Cir. 2017) (explaining that “if constitutional standing can be shown

## **B. The First Amendment**

This case requires that we apply longstanding First Amendment principles to somewhat novel facts: A popular social-media platform, subject to the control of a foreign adversary nation, that a statute requires be divested because of national security risks. The issue is made more complex by the web of subsidiaries wholly owned by ByteDance that lie behind the TikTok platform. *See Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2410 (2024) (Barrett, J., concurring) (explaining how foreign ownership and corporate structure can complicate the First Amendment analysis).

We conclude the Act implicates the First Amendment and is subject to heightened scrutiny. Whether strict or intermediate scrutiny applies is a closer question. The relevant portions of the Act are facially content neutral, but the Government arguably based its content-manipulation justification for the Act upon the content on the platform. We think it only prudent, therefore, to assume without deciding that the higher standard applies.

### **1. Heightened scrutiny applies.**

As in most First Amendment cases, the parties spend much of their time debating the appropriate standard of review. The petitioners urge the court to apply strict scrutiny but contend the Act fails intermediate scrutiny as well. The Government suggests we apply only rational basis review, alternatively advocates intermediate scrutiny, but maintains the Act satisfies even strict scrutiny.

---

for at least one plaintiff, we need not consider the standing of the other plaintiffs to raise that claim” (cleaned up)).

Under intermediate scrutiny, the Act complies with the First Amendment “if it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests.” *Turner Broad. Sys., Inc. v. FCC (Turner II)*, 520 U.S. 180, 189 (1997) (citing *United States v. O’Brien*, 391 U.S. 367, 377 (1968)). Under strict scrutiny, the Act violates the First Amendment unless the Government can “prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest.” *Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (cleaned up).

We think it clear that some level of heightened scrutiny is required. The question whether intermediate or strict scrutiny applies is difficult because the TikTok-specific provisions are facially content neutral, yet the Government justifies the Act in substantial part by reference to a foreign adversary’s ability to manipulate content seen by Americans. No Supreme Court case directly addresses whether such a justification renders a law content based, thereby triggering strict scrutiny. There are reasonable bases to conclude that intermediate scrutiny is appropriate even under these circumstances. We need not, however, definitively decide that question because we conclude the Act “passes muster even under the more demanding standard.” *FEC v. Int’l Funding Inst.*, 969 F.2d 1110, 1116 (D.C. Cir. 1992); *see also In re Sealed Case*, 77 F.4th 815, 829–30 (D.C. Cir. 2023) (assuming without deciding that strict scrutiny applied).

At the outset, we reject the Government’s ambitious argument that this case is akin to *Arcara v. Cloud Books, Inc.*, 478 U.S. 697 (1986), and does not implicate the First Amendment at all. That case concerned enforcement of “a public health regulation of general application against” an adult bookstore being “used for prostitution.” *Id.* at 707.

Enforcement of a generally applicable law unrelated to expressive activity does not call for any First Amendment scrutiny. *Id.* By contrast, the First Amendment is implicated in “cases involving governmental regulation of conduct that has an expressive element,” or when a statute is directed at an activity without an expressive component but imposes “a disproportionate burden upon those engaged in protected First Amendment activities.” *Id.* at 703–04; *see also Alexander v. United States*, 509 U.S. 544, 557 (1993).

Here the Act imposes a disproportionate burden on TikTok, an entity engaged in expressive activity. The Government concedes, as it must after *NetChoice*, that the curation of content on TikTok is a form of speech. 144 S. Ct. at 2401. Like the social media companies in that case, TikTok delivers a “personalized collection” of content to users and moderates this content pursuant to its community guidelines. *Id.* at 2403–04. The Act plainly “single[s] out” that expressive activity by indirectly subjecting TikTok — and so far, only TikTok — to the divestiture requirement. *Arcara*, 478 U.S. at 707; *cf. Nat’l Rifle Ass’n of Am. v. Vullo*, 602 U.S. 175, 190 (2024) (explaining that “the First Amendment prohibits government officials from wielding their power selectively to punish or suppress speech, directly or (as alleged here) through private intermediaries”). The prohibitions will make it unlawful for any entity to distribute, maintain, or update the TikTok platform in the United States. § 2(a)(1). TikTok can avoid the prohibitions by making a qualified divestiture, § 2(c), but to qualify such divestiture must preclude “any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing,” § 2(g)(6)(B). By prohibiting third parties from hosting TikTok until the platform executes this divestiture, the Act singles out TikTok, which engages in expressive activity, for disfavored treatment.

The Government suggests that because TikTok is wholly owned by ByteDance, a foreign company, it has no First Amendment rights. *Cf. Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 591 U.S. 430, 436 (2020) (explaining that “foreign organizations operating abroad have no First Amendment rights”). TikTok, Inc., however, is a domestic entity operating domestically. *See NetChoice*, 144 S. Ct. at 2410 (Barrett, J., concurring) (identifying potential “complexities” for First Amendment analysis posed by the “corporate structure and ownership of some platforms”). The Government does not dispute facts suggesting at least some of the regulated speech involves TikTok’s U.S. entities. *See* TikTok App. 811–12, 817–18 (explaining that promoted videos are “reviewed by a U.S.-based reviewer,” that an executive employed by a U.S. entity approves the guidelines for content moderation, and that the recommendation engine “is customized for TikTok’s various global markets” and “subject to special vetting in the United States”).

Nor does the Government argue we should “pierce the corporate veil” or “invoke any other relevant exception” to the fundamental principle of corporate separateness. *Agency for Int'l Dev.*, 591 U.S. at 435–36. We are sensitive to the risk of a foreign adversary exploiting corporate form to take advantage of legal protections in the United States. Indeed, the Government presented evidence to suggest the PRC intentionally attempts to do just that. *See, e.g.*, Gov’t App. 33–35 (describing the PRC’s hybrid commercial threat and its exploitation of U.S. legal protections for hacking operations). Under these circumstances, however, we conclude that the TikTok-specific provisions of the Act trigger First Amendment scrutiny.

The next question is whether intermediate or strict scrutiny is appropriate, which turns on whether the Act is content



neutral or content based. *See Turner Broad. Sys., Inc. v. FCC (Turner I)*, 512 U.S. 622, 642 (1994) (explaining that “regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny, because in most cases they pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue” (citation omitted)). A law is content based if it “applies to particular speech because of the topic discussed or the idea or message expressed.” *Reed*, 576 U.S. at 163. It is facially content based “if it targets speech based on its communicative content.” *City of Austin v. Reagan Nat’l Advert. of Austin, LLC*, 596 U.S. 61, 69 (2022) (cleaned up). A law that “requires an examination of speech only in service of drawing neutral, location-based lines” does not target speech based upon its communicative content. *Id.*; *see BellSouth Corp. v. FCC (BellSouth I)*, 144 F.3d 58, 69 (D.C. Cir. 1998) (applying intermediate scrutiny to a law that “defines the field of expression to which it applies by reference to a set of categories that might in a formal sense be described as content-based”). Facial neutrality, however, does not end the analysis. Even laws that are facially content neutral are content based if they (a) “cannot be justified without reference to the content of the regulated speech” or (b) “were adopted by the government because of disagreement with the message the speech conveys.” *Reed*, 576 U.S. at 164 (cleaned up).

The provisions of the Act before us are facially content neutral because they do not target speech based upon its communicative content. The TikTok-specific provisions instead straightforwardly require only that TikTok divest its platform as a precondition to operating in the United States. On its face, the Act concerns control by a foreign adversary and not “the topic discussed or the idea or message expressed.” *City of Austin*, 596 U.S. at 69 (cleaned up).

TikTok insists the TikTok-specific provisions nonetheless require strict scrutiny because they single out a particular speaker. To be sure, laws that “discriminate among media, or among different speakers within a single medium, often present serious First Amendment concerns.” *Turner I*, 512 U.S. at 659. “It would be error to conclude, however, that the First Amendment mandates strict scrutiny for any speech regulation that applies to one medium (or a subset thereof) but not others.” *Id.* at 660; *see, e.g., BellSouth I*, 144 F.3d at 68 (rejecting argument that a statute “warrants strict First Amendment review because it targets named corporations”). Strict scrutiny “is unwarranted when the differential treatment is justified by some special characteristic of the particular medium being regulated.” *Turner I*, 512 U.S. at 660–61 (cleaned up). As of now, the TikTok platform is the only global platform of its kind that has been designated by the political branches as a foreign adversary controlled application. As explained below, the Government presents two persuasive national security justifications that apply specifically to the platform that TikTok operates. “It should come as no surprise, then, that Congress decided to impose [certain restrictions] upon [TikTok] only.” *Id.* at 661.

Whether the Act, which is facially content neutral, is subject to strict scrutiny therefore turns upon the Government’s justifications for the law. *See Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (stating that a “regulation of expressive activity is content neutral so long as it is justified without reference to the content of the regulated speech” (cleaned up)); *Reed*, 576 U.S. at 164 (explaining that laws are content based if they “cannot be justified without reference to the content of the regulated speech” (cleaned up)); *City of Austin*, 596 U.S. at 76 (explaining that “an impermissible purpose or justification” may render a facially content-neutral restriction content based). The Government offers two national security justifications:

(1) to counter the PRC's efforts to collect great quantities of data about tens of millions of Americans, and (2) to limit the PRC's ability to manipulate content covertly on the TikTok platform. The former does not reference the content of speech or reflect disagreement with an idea or message. *See Ward*, 491 U.S. at 792 (finding justifications offered for a municipal noise regulation content neutral). The Government's explanation of the latter justification does, however, reference the content of TikTok's speech. Specifically, the Government invokes the risk that the PRC might shape the content that American users receive, interfere with our political discourse, and promote content based upon its alignment with the PRC's interests. In fact, the Government identifies a particular topic — Taiwan's relationship to the PRC — as a "significant potential flashpoint" that may be a subject of the PRC's influence operations, and its declarants identify other topics of importance to the PRC. Gov't Br. 22 (quoting Gov't App. 7 (Decl. of Asst. Dir. of Nat'l Intel. Casey Blackburn)); *see also* Gov't App. 9, 22.

At the same time, the Government's concern with content manipulation does not reflect "an impermissible purpose or justification." *City of Austin*, 596 U.S. at 76. On the contrary, the Government's aim is to preclude a foreign adversary from manipulating public dialogue. To that end, the Act narrowly addresses foreign adversary control of an important medium of communication in the United States. Consequently, the Government does not suppress content or require a certain mix of content. Indeed, content on the platform could in principle remain unchanged after divestiture, and people in the United States would remain free to read and share as much PRC propaganda (or any other content) as they desire on TikTok or any other platform of their choosing. What the Act targets is the PRC's ability to manipulate that content covertly. Understood

in that way, the Government’s justification is wholly consonant with the First Amendment.

Although we can conceive of reasons intermediate scrutiny may be appropriate under these circumstances, we ultimately do not rest our judgment on those reasons because the Act satisfies “the more demanding standard.” *Int’l Funding Inst.*, 969 F.2d at 1116. We therefore assume without deciding that strict scrutiny applies and uphold the law on that basis.<sup>8</sup> Our decision to resolve the case in this way follows a similar approach taken by this and other courts when faced with a government action that would satisfy strict scrutiny. *See In re Sealed Case*, 77 F.4th at 829–30; *United States v. Hamilton*, 699 F.3d 356, 371 (4th Cir. 2012); *OPAL – Bldg. AAPI Feminist Leadership v. Yost*, No. 24-3768, 2024 WL 4441458, at \*5 (6th Cir. Oct. 8, 2024); *see also Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293, 298–99 (1984) (assuming without deciding that conduct implicated the First Amendment and upholding a regulation under intermediate scrutiny); *Int’l Funding Inst.*, 969 F.2d at 1116 (assuming without deciding that intermediate scrutiny rather than rational-basis review applied); *United States v. Trump*, 88 F.4th 990, 1008 (D.C. Cir. 2023) (assuming without deciding “that the most demanding scrutiny” applied to an order restricting the speech of the defendant in a criminal trial); *cf. City of Ladue v. Gilleo*, 512 U.S. 43, 53 & n.11 (1994) (conversely assuming

---

<sup>8</sup> We agree with our concurring colleague that the Government’s data-protection rationale “is plainly content-neutral” and standing alone would at most trigger intermediate scrutiny. Concurring Op. 12–13. As we have explained, however, that is not clear for the Government’s content-manipulation justification, and no party has identified any portion of the Act to which the data justification alone applies. We therefore assume strict scrutiny applies to our review of the Act in its entirety and consider both justifications under that standard.

without deciding intermediate scrutiny rather than strict scrutiny should be applied, thereby setting “to one side the content discrimination question”).

## **2. The Act satisfies strict scrutiny.**

To satisfy strict scrutiny the Government must “demonstrate that a speech restriction: (1) serves a compelling government interest; and (2) is narrowly tailored to further that interest.” *In re Sealed Case*, 77 F.4th at 830. “A restriction is narrowly tailored if less restrictive alternatives would not accomplish the Government’s goals equally or almost equally effectively.” *Id.* (cleaned up). The Act clears this high bar.

We emphasize from the outset that our conclusion here is fact-bound. The multi-year efforts of both political branches to investigate the national security risks posed by the TikTok platform, and to consider potential remedies proposed by TikTok, weigh heavily in favor of the Act. The Government has offered persuasive evidence demonstrating that the Act is narrowly tailored to protect national security. “Given the sensitive interests in national security and foreign affairs at stake,” the Government’s judgment based upon this evidence “is entitled to significant weight.” *Holder v. Humanitarian Law Project*, 561 U.S. 1, 36 (2010). Our deference to the Government’s national-security assessment “is redoubled by the repeated acts of” the political branches to address the national security problems presented by the TikTok platform. *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 948 (D.C. Cir. 2024). The Act was the culmination of extensive, bipartisan action by the Congress and by successive presidents. It was carefully crafted to deal only with control by a foreign adversary, and it was part of a broader effort to counter a well-substantiated national security threat posed by the PRC. Under

these circumstances, the provisions of the Act that are before us withstand the most searching review.

**a. The Government’s justifications are compelling.**

Recall that the Government offers two national security justifications for the Act: to counter (1) the PRC’s efforts to collect data of and about persons in the United States, and (2) the risk of the PRC covertly manipulating content on TikTok. Each constitutes an independently compelling national security interest.

In reaching that conclusion, we follow the Supreme Court in affording great weight to the Government’s “evaluation of the facts” because the Act “implicates sensitive and weighty interests of national security and foreign affairs.” *Humanitarian Law Project*, 561 U.S. at 33–34; *Trump v. Hawaii*, 585 U.S. 667, 707–08 (2018) (same); *see, e.g., Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1162, 1164 (D.C. Cir. 2023) (declining to second-guess the Executive’s judgment regarding a national security threat posed by the PRC). At the same time, of course, we “do not defer to the Government’s reading of the First Amendment.” *Humanitarian Law Project*, 561 U.S. at 34. We simply recognize the comparatively limited competence of courts at “collecting evidence and drawing factual inferences in this area.” *Id.* With regard to national security issues, the political branches may — and often must — base their actions on their “informed judgment,” which “affects what we may reasonably insist on from the Government.” *Id.* at 34–35.

(i) *National security justifications*

The Government provides persuasive support for its concerns regarding the threat posed by the PRC in general and

through the TikTok platform in particular. As Assistant Director of National Intelligence Casey Blackburn explained, the “PRC is the most active and persistent cyber espionage threat to U.S. government, private-sector, and critical infrastructure networks.” Its hacking program “spans the globe” and “is larger than that of every other major nation, combined.” The PRC has “pre-positioned” itself “for potential cyber-attacks against U.S. critical infrastructure by building out offensive weapons within that infrastructure.” Consistent with that assessment, the Government “has found persistent PRC access in U.S. critical telecommunications, energy, water, and other infrastructure.” See *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256, 262–63 (D.C. Cir. 2022) (describing the Government’s shift in focus from terrorism to PRC “cyber threats” and the risk posed by use of PRC-connected “information technology firms as systemic espionage platforms”). “The FBI now warns that no country poses a broader, more severe intelligence collection threat than China.” *Id.* at 263.

Of particular relevance to the Government’s first justification for the Act, the PRC has engaged in “extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations.” It has done so through hacking operations, such as by penetrating the U.S. Government Office of Personnel Management’s systems and taking “reams” of personal data, stealing financial data on 147 million Americans from a credit-reporting agency, and “almost certainly” extracting health data on nearly 80 million Americans from a health insurance provider.

The PRC’s methods for collecting data include using “its relationships with Chinese companies,” making “strategic investments in foreign companies,” and “purchasing large data sets.” For example, the PRC has attempted “to acquire sensitive

health and genomic data on U.S. persons” by investing in firms that have or have access to such data. Government counterintelligence experts describe this kind of activity as a “hybrid commercial threat.”

The PRC poses a particularly significant hybrid commercial threat because it has adopted laws that enable it to access and use data held by Chinese companies. *See China Telecom (Ams.) Corp.*, 57 F.4th at 263 (describing the legal framework through which the PRC has “augmented the level of state control over the cyber practices of Chinese companies”). For example, the National Security Law of 2015 requires all citizens and corporations to provide necessary support to national security authorities. Similarly, the Cybersecurity Law of 2017 requires Chinese companies to grant the PRC full access to their data and to cooperate with criminal and security investigations.

The upshot of these and other laws, according to the Government’s declarants, is that “even putatively ‘private’ companies based in China do not operate with independence from the government and cannot be analogized to private companies in the United States.” Through its “control over Chinese parent companies,” the PRC can also “access information from and about U.S. subsidiaries and compel their cooperation with PRC directives.” As a result, the PRC can “conduct espionage, technology transfer, data collection, and other disruptive activities under the disguise of an otherwise legitimate commercial activity.” According to Kevin Vorndran, Assistant Director of the FBI’s Counterintelligence Division, the PRC endeavors strategically to pre-position commercial entities in the United States that the PRC can later “co-opt.” These pre-positioning “tactics can occur over the span of several years of planning and implementation, and they



are one “part of the PRC’s broader geopolitical and long-term strategy to undermine U.S. national security.”

The PRC likewise uses its cyber capabilities to support its influence campaigns around the world. Those global “influence operations” aim to “undermine democracy” and “extend the PRC’s influence abroad.” Specifically, the PRC conducts “cyber intrusions targeted to affect U.S. and non-U.S. citizens beyond its borders — including journalists, dissidents, and individuals it views as threats — to counter and suppress views it considers critical of [the PRC].” Notably, the Government reports that “ByteDance and TikTok Global have taken action in response to PRC demands to censor content *outside* of China.”

As it relates to TikTok in the United States, the Government predicts that ByteDance and TikTok entities “would try to comply if the PRC asked for specific actions to be taken to manipulate content for censorship, propaganda, or other malign purposes on TikTok US.” The Government says that ByteDance, which is subject to PRC laws requiring cooperation with the PRC, could do so by acting unilaterally or by conscripting its U.S. entities. The former conclusion is evidenced by the fact that the PRC maintains a powerful Chinese Communist Party committee “embedded in ByteDance” through which it can “exert its will on the company.” As of 2022, that committee “was headed by the company’s chief editor and comprised at least 138 employees at its Beijing office, including senior company managers.” The latter conclusion is supported by the fact that TikTok’s U.S. operations are “heavily reliant” on ByteDance. As TikTok’s declarants have put it, “TikTok in the United States is an integrated part of the global platform” supported by teams “spread across several different corporate entities and countries,” and TikTok is “highly integrated with ByteDance.”

The Government also identifies several public reports, which were considered by the Congress prior to passing the Act, regarding the risks posed by TikTok.<sup>9</sup> For example, a Government declarant points to “reporting by Forbes Magazine” to illustrate in part why the Government did not trust TikTok’s proposed mitigation measures. The reporting suggested “that ByteDance employees abused U.S. user data, even after the establishment of TTUSDS,” and drew attention to “audio recordings of ByteDance meetings” that indicated “ByteDance retained considerable control and influence over TTUSDS operations.” In its report recommending passage of the Act, a committee of the Congress collected “a list of public statements that have been made regarding the national security risks posed by . . . TikTok.” H.R. Rep. No. 118-417, at 5–12 (2024). According to the committee, public reporting suggested that TikTok had stored sensitive information about U.S. persons (including “Social Security numbers and tax identifications”) on servers in China; TikTok’s “China-based employees” had “repeatedly accessed non-public data about U.S. TikTok users”; ByteDance employees had “accessed TikTok user data and IP addresses to monitor the physical locations of

---

<sup>9</sup> Although our disposition of this case does not turn upon these reports, the Congress and the President obviously were entitled to consider such materials when deciding whether to define TikTok as a foreign adversary controlled application under the Act. Indeed, we have “approved” the use of similar public materials by the President when making decisions to designate people or entities under various national-security related statutes. *See Zevallos v. Obama*, 793 F.3d 106, 109, 113 (2015) (finding it “clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations” (quoting *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 162 (2003) (regarding designation of an entity as a Specially Designated Global Terrorist))).

specific U.S. citizens”; and PRC agents had inspected “TikTok’s internal platform.” *Id.* at 7–10.

The resulting judgment of the Congress and the Executive regarding the national security threat posed by the TikTok platform “is entitled to significant weight, and we have persuasive evidence [in the public record] before us to sustain it.” *Humanitarian Law Project*, 561 U.S. at 36. The petitioners raise several objections to each national security justification, which we take up next, but the bottom line is that they fail to overcome the Government’s considered judgment and the deference we owe that judgment.

(ii) *Data collection*

TikTok disputes certain details about the Government’s concern with its collection of data on U.S. persons but misses the forest for the trees. The TikTok platform has more than 170 million monthly users in the United States. It is an immensely popular platform on which users in the United States have uploaded more than 5.5 billion videos in a single year. According to TikTok’s “privacy policy,” TikTok automatically collects large swaths of data about its users, including device information (IP address, keystroke patterns, activity across devices, browsing and search history, etc.) and location data (triangulating SIM card or IP address data for newer versions of TikTok and GPS information for older versions). TikTok, *Privacy Policy*, <https://perma.cc/E36Q-M3KS> (last updated Aug. 19, 2024). It may also collect image and audio information (including biometric identifiers and biometric information such as faceprints and voiceprints); metadata (describing how, when, where, and by whom content was created, collected, or modified); and usage information (including content that users upload to TikTok). *Id.* That is not to mention information that users voluntarily provide, such as name, age,

username, password, email, phone number, social media account information, messages exchanged on the platform and, “with your permission,” your “phone and social network contacts.” *Id.* TikTok’s “privacy policy” also makes clear that it uses these data to “infer additional information” about its users. Given the magnitude of the data gathered by TikTok and TikTok’s connections to the PRC, two consecutive presidents understandably identified TikTok as a significant vulnerability. Access to such information could, for example, allow the PRC to “track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.” *Addressing the Threat Posed by TikTok*, 85 Fed. Reg. at 48637.

TikTok does not deny that it collects a substantial amount of data on its users. Instead TikTok disputes details about the Government’s understanding of its data practices and questions the sincerity of the Government’s data justification. At the same time, however, TikTok’s own declarants provide support for the Government’s concern. They emphasize the integrated nature of the TikTok platform to argue that divestiture would be infeasible. They argue that prohibiting data sharing between TikTok in the United States and “the entities that operate the global platform” would make TikTok uncompetitive with “rival, global platforms.” They also acknowledge that, even under TikTok’s proposed NSA, ByteDance would continue to have access to some Protected Data on TikTok users in the United States through “limited access protocols.” They likewise state that TikTok’s proposed NSA “does allow for TTUSDS and Oracle to send ‘Excepted Data’ to ByteDance.”

Set against those statements, TikTok’s arguments concerning the specific data collected and TikTok’s voluntary data protection efforts fall flat. For example, TikTok quibbles with the Government’s stated concern that TikTok collects data

on users’ “precise locations, viewing habits, and private messages,” including “data on users’ phone contacts who do not themselves use TikTok.” Gov’t Br. 1; *see* TikTok Reply Br. 25. According to a TikTok declarant, the current version of TikTok can only “approximate users’ geographic locations.” Access to a user’s contact list, likewise, is currently available only if a user affirmatively opts in, and it is “anonymized and used only to facilitate connections with other TikTok users.” TikTok Reply Br. 25. TikTok further points to other data protections that it claims to provide, such as storing sensitive user data in the United States and controlling access to them.

The Government’s data-related justification for the Act, however, does not turn on the details of TikTok’s mitigation measures. Even after extended negotiations, TikTok could not satisfactorily resolve the Government’s concerns. We have no doubt, and the Government has never denied, that TikTok’s proposed NSA would mitigate the Government’s concerns to some extent. Nor do we doubt that TikTok’s voluntary mitigation efforts provide some protection. The problem for TikTok is that the Government exercised its considered judgment and concluded that mitigation efforts short of divestiture were insufficient, as a TikTok declarant puts it, to mitigate “risks to acceptable levels.” At bottom, the Government lacks confidence that it has sufficient visibility and resources to monitor TikTok’s promised measures, nor does it have “the requisite trust” that “ByteDance and TTUSDS would comply in good faith.” The court can neither fault nor second guess the Government on these crucial points.

This situation is much like that in *Pacific Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023), which involved the Executive’s decision to revoke authorizations held by PRC-controlled companies to operate communication lines in the United States. There, as here, the PRC indirectly controlled the

companies “through a web of foreign affiliates.” 77 F.4th at 1163 (cleaned up). The Executive “concluded that China’s ownership raised significant concerns that the [companies] would be forced to comply with Chinese government requests.” *Id.* (cleaned up). The Government was concerned that the PRC could “access, monitor, store, and in some cases disrupt or misroute U.S. communications, which in turn [would] allow them to engage in espionage and other harmful activities against the United States.” *Id.* (cleaned up). The Executive “further concluded that the [companies] had shown a lack of candor and trustworthiness” and therefore “nothing short of revocation would ameliorate the national-security risks.” *Id.* This court declined the appellants’ invitation to “second-guess” the Executive’s judgment regarding the threat to national security. *Id.* at 1164. We also upheld the Executive’s conclusion that the companies’ “untrustworthiness would make any mitigation agreement too risky” in part because the Executive could not “comprehensively monitor compliance” or “reliably detect surreptitious, state-sponsored efforts at evasion.” *Id.* at 1165–66. The same considerations similarly support the Government’s judgment here.

We also reject TikTok’s argument that the Government’s data-related concerns are speculative. The Government “need not wait for a risk to materialize” before acting; its national security decisions often must be “based on informed judgment.” *China Telecom (Ams.) Corp.*, 57 F.4th at 266. Here the Government has drawn reasonable inferences based upon the evidence it has. That evidence includes attempts by the PRC to collect data on U.S. persons by leveraging Chinese-company investments and partnerships with U.S. organizations. It also includes the recent disclosure by former TikTok employees that TikTok employees “share U.S. user data on PRC-based internal communications systems that China-based ByteDance employees can access,” and that the ByteDance subsidiary

responsible for operating the platform in the United States “approved sending U.S. data to China several times.” In short, the Government’s concerns are well founded, not speculative.

TikTok next contends that, because other companies with operations in China collect data in the United States, its data collection is not the Government’s real concern. As already explained, however, the Act complements the Data Broker Law, which limits the access of any foreign adversary country (or entity controlled by such a country) to data from third-party brokers. The Act also includes a generally applicable framework through which the Executive can address other foreign adversary controlled applications in the future. That the Act does not fully solve the data collection threat posed by the PRC does not mean it was not a step in the right direction. Moreover, TikTok does not identify any company operating a comparable platform in the United States with equivalent connections to the PRC. Nor would it be dispositive if TikTok had done so because the political branches are free to “focus on their most pressing concerns.” *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 449 (2015). The Government’s multi-year efforts to address the risks posed by the TikTok platform support the conclusion that TikTok was, in fact, the Government’s most pressing concern.

(iii) *Content manipulation*

Preventing covert content manipulation by an adversary nation also serves a compelling governmental interest. The petitioners object for two reasons, neither of which persuades.

First, TikTok incorrectly frames the Government’s justification as suppressing propaganda and misinformation. The Government’s justification in fact concerns the risk of the PRC covertly manipulating content on the platform. For that reason, again, the Act is directed only at control of TikTok by

a foreign adversary nation. At points, TikTok also suggests the Government does not have a legitimate interest in countering covert content manipulation by the PRC. To the extent that is TikTok’s argument, it is profoundly mistaken. “At the heart of the First Amendment lies the principle that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence. Our political system and cultural life rest upon this ideal.” *Turner I*, 512 U.S. at 641. When a government — domestic or foreign — “stifles speech on account of its message . . . [it] contravenes this essential right” and may “manipulate the public debate through coercion rather than persuasion.” *Id.*; see also *Nat’l Rifle Ass’n of Am.*, 602 U.S. at 187 (explaining that at the core of the First Amendment “is the recognition that viewpoint discrimination is uniquely harmful to a free and democratic society”).

In this case, a foreign government threatens to distort free speech on an important medium of communication. Using its hybrid commercial strategy, the PRC has positioned itself to manipulate public discourse on TikTok in order to serve its own ends. The PRC’s ability to do so is at odds with free speech fundamentals. Indeed, the First Amendment precludes a domestic government from exercising comparable control over a social media company in the United States. See *NetChoice*, 144 S. Ct. at 2407 (explaining that a state government “may not interfere with private actors’ speech” because the First Amendment prevents “the government from tilting public debate in a preferred direction” (cleaned up)). Here the Congress, as the Executive proposed, acted to end the PRC’s ability to control TikTok. Understood in that way, the Act actually vindicates the values that undergird the First Amendment.

Like the Supreme Court, “We also find it significant that [the Government] has been conscious of its own responsibility to consider how its actions may implicate constitutional



concerns.” *Humanitarian Law Project*, 561 U.S. at 35. Rather than attempting itself to influence the content that appears on a substantial medium of communication, the Government has acted solely to prevent a foreign adversary from doing so. As our concurring colleague explains, this approach follows the Government’s well-established practice of placing restrictions on foreign ownership or control where it could have national security implications. Concurring Op. 2–5; *see* 47 U.S.C. § 310(a)–(b) (restricting foreign control of radio licenses); *Pac. Networks Corp.*, 77 F.4th at 1162 (upholding the FCC’s decision to revoke authorizations to operate communications lines); *Moving Phones P’ship v. FCC*, 998 F.2d 1051, 1055, 1057 (D.C. Cir. 1993) (upholding the Executive’s application of the Communications Act’s “ban on alien ownership” of radio licenses “to safeguard the United States from foreign influence in broadcasting” (cleaned up)); *see also Palestine Info. Off. v. Shultz*, 853 F.2d 932, 936, 945 (D.C. Cir. 1988) (upholding the Executive’s divestiture order under the Foreign Missions Act regarding an organization the activities of which “were deemed inimical to America’s interests”); 49 U.S.C. § 40102(a)(2), (15) (requiring that a U.S. “air carrier” be “under the actual control of citizens of the United States”).

Consequently, the Act is not, as the User Petitioners suggest, an effort to “control the flow of ideas to the public.” *Lamont v. Postmaster Gen.*, 381 U.S. 301, 306–07 (1965). Nor are the User Petitioners correct to characterize the TikTok-specific provisions as a prior restraint on speech or an infringement on associational rights. Were a divestiture to occur, TikTok Inc.’s new owners could circulate the same mix of content as before without running afoul of the Act. People in the United States could continue to engage with content on TikTok as at present. The only change worked by the Act is that the PRC could not “manipulate the public debate through coercion rather than persuasion.” *Turner I*, 512 U.S. at 641.

TikTok resists this conclusion by emphasizing stray comments from the congressional proceedings that suggest some congresspersons were motivated by hostility to certain content. The Supreme Court, however, has repeatedly instructed that courts should “not strike down an otherwise constitutional statute on the basis of an alleged illicit legislative motive.” *O’Brien*, 391 U.S. at 383; *City of Renton v. Playtime Theaters, Inc.*, 475 U.S. 41, 47–49 (1986) (rejecting speculation about the “motivating factor” behind an ordinance justified without reference to speech); *Turner I*, 512 U.S. at 652 (similar). The Act itself is the best evidence of the Congress’s and the President’s aim. The narrow focus of the Act on ownership by a foreign adversary and the divestiture exemption provide convincing evidence that ending foreign adversary control, not content censorship, was the Government’s objective.

The petitioners nevertheless contend the divestiture provisions and an exclusion from the generally applicable track betray the Government’s real purpose to ban TikTok as a means of censoring content. They claim the divestiture exemption cannot be satisfied in the time allowed by the Act, which effectively makes it a ban. Conversely, they argue an exclusion from the definition of “covered company” — for entities that operate an “application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews,” § 2(g)(2)(B) — creates a loophole to the generally applicable track so large that no other company is likely ever to be subjected to the prohibitions of the Act.<sup>10</sup> The upshot, according to TikTok, is that the Congress

---

<sup>10</sup> The parties offer competing interpretations of this exclusion. Because we do not doubt the Government’s “proffered . . . interest actually underlies the law” under either interpretation, we have no occasion to interpret that provision in this case. *Blount v. SEC*, 61 F.3d 938, 946 (D.C. Cir. 1995) (quotation omitted).

“purpose-built the Act to ban TikTok because it objects to TikTok’s content.” TikTok Reply Br. 28.

We discern no such motive from the divestiture provisions or the design of the generally applicable framework. Although the Government does not rebut TikTok’s argument that 270 days is not enough time for TikTok to divest given its high degree of integration with ByteDance, 270 days is a substantial amount of time. If TikTok (or any company subject to the Act) is unable to divest within 270 days, it can do so later and thereby lift the prohibitions. § 2(c)(1)(A)–(B). Consequently, we detect no illicit motive on the part of the Congress to ban TikTok and suppress its speech by means of the divestiture provisions.

The same is true of the reviews exclusion, which appears to reflect a good-faith effort by the Congress to narrow the scope of the general track to applications the Congress determined to present the greatest risks to national security. That the Congress created a new mechanism by which the Executive can counter threats similar to TikTok in the future — and excluded a category of applications from that framework — does not suggest the Congress’s national security concerns specific to TikTok were a charade. In fact, the Congress was not required to include a generally applicable framework at all; it could have focused only on TikTok. *See Williams-Yulee*, 575 U.S. at 452 (“The First Amendment does not put [the Congress] to [an] all-or-nothing choice”). The Congress was entitled to address the threat posed by TikTok directly and create a generally applicable framework, however imperfect, for future use. It would be inappropriate to “punish” the Congress for attempting to address future national security threats by inferring an impermissible motive. *Id.*

Second, TikTok contends the Government's content-manipulation rationale is speculative and based upon factual errors. TikTok fails, however, to grapple fully with the Government's submissions. On the one hand, the Government acknowledges that it lacks specific intelligence that shows the PRC has in the past or is now coercing TikTok into manipulating content in the United States. On the other hand, the Government is aware "that ByteDance and TikTok Global have taken action in response to PRC demands to censor content *outside* of China." The Government concludes that ByteDance and its TikTok entities "have a demonstrated history of manipulating the content on their platforms, including at the direction of the PRC." Notably, TikTok never squarely denies that it has ever manipulated content on the TikTok platform at the direction of the PRC. Its silence on this point is striking given that "the Intelligence Community's concern is grounded in the actions ByteDance and TikTok have already taken overseas." It may be that the PRC has not yet done so in the United States or, as the Government suggests, the Government's lack of evidence to that effect may simply reflect limitations on its ability to monitor TikTok.

In any event, the Government reasonably predicts that TikTok "would try to comply if the PRC asked for specific actions to be taken to manipulate content for censorship, propaganda, or other malign purposes" in the United States. That conclusion rests on more than mere speculation. It is the Government's "informed judgment" to which we give great weight in this context, even in the absence of "concrete evidence" on the likelihood of PRC-directed censorship of TikTok in the United States. *Humanitarian Law Project*, 561 U.S. at 34–35.

The purported factual errors identified by TikTok do not alter that conclusion. TikTok principally faults the Government

for claiming the recommendation engine is “based in China” because it now resides in the Oracle cloud. TikTok Reply Br. 21–22. No doubt, but the Government’s characterization is nonetheless consistent with TikTok’s own declarations. TikTok’s declarants explained that now and under its proposed NSA “ByteDance will remain completely in control of developing the Source Code for all components that comprise ‘TikTok’ . . . including the Recommendation Engine.” They likewise represent that TikTok presently “relies on the support of employees of other ByteDance subsidiaries” for code development. Even when TikTok’s voluntary mitigation measures have been fully implemented, the “source code supporting the TikTok platform, including the recommendation engine, will continue to be developed and maintained by ByteDance subsidiary employees, including in the United States and in China.” TikTok is therefore correct to say the recommendation engine “is stored in the Oracle cloud,” but gains nothing by flyspecking the Government’s characterization of the recommendation engine still being in China.

**b. The Act is narrowly tailored.**

The TikTok-specific provisions of the Act are narrowly tailored to further the Government’s two national security interests. “It bears emphasis that, under the strict-scrutiny standard, a restriction must be narrowly tailored, not perfectly tailored.” *In re Sealed Case*, 77 F.4th at 830–31 (cleaned up). Here the relevant provisions of the Act apply narrowly because they are limited to foreign adversary control of a substantial medium of communication and include a divestiture exemption. By structuring the Act in this way, the Congress addressed precisely the harms it seeks to counter and only those harms. Moreover, as already explained, the Act’s emphasis on ownership and control follows a longstanding approach to counter foreign government control of communication media

in the United States. *E.g.*, *Pac. Networks Corp.*, 77 F.4th at 1162; *Moving Phones P'ship*, 998 F.2d at 1055–56. The petitioners argue nonetheless that there are less restrictive alternatives available and contend the Act is fatally both overinclusive and underinclusive.

(i) *TikTok's proposed NSA*

TikTok presents its proposed NSA as a less restrictive alternative. TikTok contends that, at minimum, our consideration of this alternative implicates factual disputes that require additional proceedings. TikTok, however, misapprehends the thrust of the Government's objection to the proposed NSA. A senior Executive Branch official involved in the negotiations provided several reasons for which the Executive rejected the proposal. These included lack of U.S. visibility into PRC activity, the Executive's inability to monitor compliance with the NSA, and therefore its inadequate ability to deter non-compliance; insufficient operational independence for TikTok; and insufficient data protections for Americans. Moreover, and "most fundamentally," the NSA "still permitted certain data of U.S. users to flow to China, still permitted ByteDance executives to exert leadership control and direction over TikTok's US operations, and still contemplated extensive contacts between the executives responsible for the TikTok U.S. platform and ByteDance leadership overseas." At bottom, acceptance of "the Final Proposed NSA would ultimately have relied on the Executive Branch trusting ByteDance" to comply with the agreement, which the Government understandably judged it could not do. Based upon this array of problems, the Executive rejected the proposal and pursued a legislative solution.

TikTok adamantly disagrees with the Executive's judgment. It is not, however, the job of the petitioners or of the

courts to substitute their judgments for those of the political branches on questions of national security. *See Hernández v. Mesa*, 589 U.S. 93, 113 (2020). Understandably, TikTok therefore attempts to couch its disagreement in factual terms. But TikTok does not present any truly material dispute of fact.

Consider, for example, TikTok’s claim that data anonymization under TikTok’s proposed NSA would effectively mitigate the Government’s concerns. The Government does not dispute that TikTok’s proposal provides for data anonymization; rather, it deems this protection vulnerable to circumvention and therefore insufficient to resolve the Government’s data-related concerns. That is a dispute of judgment not of fact. A similar point applies to the parties’ disagreement regarding the feasibility of Oracle reviewing TikTok’s source code for the Government. TikTok’s declarant says Oracle could apply methods consistent with industry standards to streamline that review and points out that TikTok’s proposed NSA would require Oracle to conduct its initial review in 180 days. The Government does not disagree; rather, it doubts the adequacy of Oracle’s review of the source code — notwithstanding “Oracle’s considerable resources” — based upon extensive technical conversations with Oracle. Moreover, even after “assuming every line of Source Code could be monitored and verified,” the Government still concluded that “the PRC could exert malign influence” through commercial features of the platform that would not be identified through a review of the code. TikTok’s disagreement with the Government boils down to a dispute about the sufficiency of Oracle’s review to mitigate threats posed by the PRC, which is a matter of judgment, not of fact.

The same is true regarding the role of TTUSDS in limiting the PRC’s ability to control TikTok through ByteDance. The Government concludes that TTUSDS would be insufficiently

independent of ByteDance, fears TTUSDS could be pressured to do the latter's bidding, and doubts TTUSDS could prevent interference by ByteDance. Indeed, the Government predicts that "TTUSDS personnel here would not resist demands to comply" with directives "even if aware of pressure from the PRC government." Whether TTUSDS sufficiently mitigates the risk of PRC interference through ByteDance is ultimately an issue of judgment, not of fact.

Similarly, the parties' dispute about the adequacy of the temporary shutdown option — or "kill switch" — under the NSA centers on the Government's ultimate conclusion regarding the sufficiency of that option. The Government's declarant on this point explains that the "temporary stop would not . . . give the U.S. Government anything resembling complete discretion to shut down the TikTok platform based on its own independent assessment of national security risk and assessments from the U.S. Intelligence Community." TikTok's declarant, by contrast, characterizes the so-called "kill switch" as a "unilateral remedy" of unparalleled "magnitude in a CFIUS mitigation agreement," which could be applied by the Government if TikTok deployed unreviewed source code or if TikTok violates the protocols for handling Protected Data. Rhetoric aside, the substance of TikTok's objection is the Government's ultimate conclusion that the shutdown option would not adequately address the Government's concerns because of the limited scope of the shutdown option as well as the Government's inability to monitor TikTok.

In sum, even if we resolved every supposed factual dispute in TikTok's favor, the result would be the same. For us to conclude the proposed NSA is an equally or almost equally effective but less restrictive alternative, we would have to reject the Government's risk assessment and override its ultimate judgment. That would be wholly inappropriate after Executive



Branch officials “conducted dozens of meetings,” considered “scores of drafts of proposed mitigation terms,” and engaged with TikTok as well as Oracle for more than two years in an effort to work out an acceptable agreement. Here “respect for the Government’s conclusions is appropriate.” *Humanitarian Law Project*, 561 U.S. at 34.

The petitioners attempt to draw a distinction between the Executive’s rejection of the proposed NSA and the Congress’s deliberations prior to passing the Act. The petitioners complain the Congress failed even to consider TikTok’s proposed NSA. Because the Act applies narrowly to the TikTok platform, TikTok goes so far as to argue the Congress was required to make legislative findings to explain its rationale for passing the Act. These objections are unavailing. The Congress “is not obligated, when enacting its statutes, to make a record of the type that an administrative agency or court does to accommodate judicial review.” *Time Warner Entm’t Co. v. FCC*, 93 F.3d 957, 976 (D.C. Cir. 1996) (cleaned up); *Sable Commc’ns of Cal., Inc. v. FCC*, 492 U.S. 115, 133 (1989) (Scalia, J., concurring) (“Neither due process nor the First Amendment requires legislation to be supported by committee reports, floor debates, or even consideration, but only by a vote”). Moreover, the petitioners cannot credibly claim the Congress was any less aware than the Executive of the proposed NSA as a potential alternative. Prior to passage of the Act, while the Executive was negotiating the proposed NSA with TikTok, Executive Branch officials briefed congressional committees several times. The record shows that congresspersons were aware of TikTok’s voluntary mitigation efforts; TikTok and its supporters, including the PRC itself, lobbied the Congress not to pass the Act; and TikTok displayed “a pop-up message urging users to contact their representatives about the Act,” which prompted a deluge of calls to congresspersons. We think it clear the

Congress did not reject the proposed NSA for lack of familiarity; like the Executive, the Congress found it wanting.

To qualify as a less restrictive alternative, the proposed NSA must “accomplish the Government’s goals equally or almost equally effectively.” *In re Sealed Case*, 77 F.4th at 830 (cleaned up). As already stated, the Government has offered considerable evidence that the NSA would not resolve its national security concerns. Divestiture, by contrast, clearly accomplishes both goals more effectively than would the proposed NSA. It has the added virtue of doing so with greater sensitivity to First Amendment concerns by narrowly mandating an end to foreign adversary control. The proposed NSA, by contrast, contemplates an oversight role for the U.S. Government that includes what TikTok calls a “kill switch remedy” and the Government characterizes as “temporary stop” authority over the platform. Entangling the U.S. government in the daily operations of a major communications platform would raise its own set of First Amendment questions. Indeed, it could be characterized as placing U.S. government “officials astride the flow of [communications],” the very arrangement excoriated in *Lamont*, 381 U.S. at 306. Divestiture poses no such difficulty.

(ii) *Other options*

The petitioners suggest a variety of other options that the Government also found inadequate. These include disclosure or reporting requirements, the Government using speech of its own to counter any alleged foreign propaganda, limiting TikTok’s collection of location and contact data, and extending the ban of TikTok on government devices to government employees’ personal devices. None would “accomplish the Government’s goals equally or almost equally effectively.” *In re Sealed Case*, 77 F.4th at 830 (cleaned up).

The first two suggestions obviously fall short. As the Government points out, covert manipulation of content is not a type of harm that can be remedied by disclosure. The idea that the Government can simply use speech of its own to counter the risk of content manipulation by the PRC is likewise naïve. Moreover, the petitioners' attempt to frame the use of Government speech as a means of countering "alleged foreign propaganda," Creator Br. 54, is beside the point. It is the "secret manipulation of the content" on TikTok — not foreign propaganda — that "poses a grave threat to national security." Gov't Br. 36. No amount of Government speech can mitigate that threat nearly as effectively as divestiture.

The petitioners' other proposals are similarly flawed. Creators' contention that the Government "could simply ban TikTok from collecting . . . location and contact data" fundamentally misapprehends the Government's data-collection concerns, which are not limited to two types of data. Creator Reply Br. 29. The data-collection risks identified by the Government include the PRC's ability to use TikTok for "bulk collection of data" and for "targeted collection on individuals." Gov't Br. 48. Indeed, the FBI has specifically assessed that "TikTok could facilitate the PRC's access to U.S. users' data, which could enable PRC espionage, technology transfer, data collection and influence activities." For example, the PRC could use TikTok data to enhance its "artificial intelligence capabilities" and obtain "extensive information about users and non-users, including U.S. Government and U.S. intelligence community employees, U.S. political dissidents, and other individuals of interest to the PRC." Moreover, even if the Government's concerns were limited to certain categories of data, its inability to monitor TikTok makes a targeted prohibition on the collection of specific types of data less effective than divestiture.

For similar reasons, a limited prohibition addressing government employees would not suffice. The Government's concern extends beyond federal employees to "family members or potential future government employees (many of whom may be teenagers today, a particular problem given TikTok's popularity among young people)." Indeed, as the Government emphasizes, the Congress was legislating "in the interest of all Americans' data security." Gov't Br. 58. A more limited prohibition would not be as effective as divestiture.

The User Petitioners also identify as options various legislative proposals, such as the Adversarial Platform Prevention Act of 2021, S. 47, 117th Cong. (2021); Internet Application I.D. Act, H.R. 4000, 117th Cong. (2021); and the TELL Act, H.R. 742, 118th Cong. (2023), that the Congress did not adopt. In substance, these proposals are similar to the alternatives we just considered and found less effective than divestiture. If anything, those unenacted lesser legislative proposals undermine rather than advance the User Petitioners' preferred alternatives: That the Congress considered a series of other measures before ultimately adopting the Act implies only that the Congress determined nothing short of divestiture would sufficiently avoid the risks posed by TikTok.

In short, the petitioners suggest an array of options none of which comes close to serving either, much less both, the Government's goals as effectively as does divestiture. Each consequently fails to qualify as a less restrictive alternative for purposes of the First Amendment.

(iii) *Overinclusive / underinclusive*

The petitioners contend the Act is both overinclusive and underinclusive. They argue the Act is overinclusive primarily because the TikTok-specific provisions apply to another ByteDance product, CapCut, that can be used to edit videos on

various platforms including TikTok but does not collect user data or present an opportunity for PRC manipulation of content. Given the Government's well-supported concerns about ByteDance, it was necessary for the Act to apply to all ByteDance entities. Moreover, the petitioners fail to demonstrate that neither of the Government's two national security concerns implicate CapCut. We therefore conclude the TikTok-specific provisions of the Act are not overinclusive.

We likewise conclude the Act is not fatally underinclusive. The main purpose of inquiring into underinclusiveness is "to ensure that the proffered state interest actually underlies the law." *Nat'l Ass'n of Mfrs. v. Taylor*, 582 F.3d 1, 17 (D.C. Cir. 2009) (cleaned up). For that reason, underinclusiveness is fatal to a regulation only "if it cannot fairly be said to advance any genuinely substantial governmental interest, because it provides only ineffective or remote support for the asserted goals, or limited incremental support." *Id.* (cleaned up). As already explained, the Congress's decision separately and more immediately to address TikTok, the Executive's "most pressing" cause for concern, was permissible. *See Williams-Yulee*, 575 U.S. at 449. That would be so even if the Congress had not included the generally applicable framework to deal with other foreign adversary controlled platforms or had not passed the Data Broker Law alongside the Act. That the Government did both supports our conclusion that the Act reflects a good-faith effort on the part of the Government to address its national security concerns.

\* \* \*

To summarize our First Amendment analysis: The Government has provided two national security justifications for the Act. We assumed without deciding the Act is subject to strict scrutiny and we now uphold the TikTok-specific portions of the Act under each justification. This conclusion is supported by ample evidence that the Act is the least restrictive means of advancing the Government’s compelling national security interests.

### C. Equal Protection

TikTok argues that the Act violates its right to the equal protection of the laws because it singles out TikTok for disfavored treatment relative to other similarly situated platforms. The Government contends its justifications for the Act satisfy the requirement of equal protection and add that TikTok received more process than a company would receive under the generally applicable provisions. We conclude the Act is consistent with the requirement of equal protection.

“In equal protection challenges the critical question is always whether there is an appropriate governmental interest suitably furthered by the differential treatment at issue.” *Cnty-Serv. Broad. of Mid-Am., Inc. v. FCC*, 593 F.2d 1102, 1122 (D.C. Cir. 1978) (cleaned up). This question “lies at the intersection” of equal protection and the First Amendment. *News Am. Pub., Inc. v. FCC*, 844 F.2d 800, 804 (D.C. Cir. 1988) (cleaned up).

Although we review “conventional economic legislation” under a “minimum rationality” standard, *id.* at 802, we have held something “more is required than ‘minimum rationality’” when a regulation burdens “a single publisher/broadcaster,” *id.* at 814. *See also BellSouth I*, 144 F.3d at 68 (explaining that

*News America* does not require strict scrutiny for “statutes singling out particular persons for speech restrictions”); *Cnty-Serv. Broad. of Mid-Am., Inc.*, 593 F.2d at 1122 (applying to a “statute affecting First Amendment rights” an “equal protection standard [that] is closely related to the O’Brien First Amendment tests”). Having concluded the relevant parts of the Act do not violate the First Amendment even when subjected to heightened scrutiny, we readily reach the same conclusion when analyzing the Act in equal protection terms.

TikTok’s equal protection argument boils down to pointing out that TikTok alone is singled out by name in the Act, unlike companies that in the future may be subject to the generally applicable provisions of the Act. Merely singling a company out, however, does not amount to an equal protection violation if doing so furthers an appropriate governmental interest. The controlling question is “whether there is an appropriate governmental interest suitably furthered by the differential treatment at issue.” *Cnty-Serv. Broad. of Mid-Am., Inc.*, 593 F.2d at 1122–23 (holding statute violated First and Fifth Amendments by unjustifiably burdening only non-commercial broadcasters). Here the Government justified the Act by presenting two national security risks specific to the TikTok platform. By naming TikTok in the Act, the Congress ensured TikTok-related risks were addressed promptly. Simultaneously creating a generally applicable framework gave the Executive a tool to address similar risks that may come to light in the future. This differential treatment furthers the Government’s national security interest in countering the immediate threat posed by the PRC’s control of TikTok.

The governmental interests here also stand in stark contrast to the case upon which TikTok primarily relies, in which the “sole apparent difference” in treatment between similarly situated broadcasters was due to “an accident of timing.” *News*

*Am. Pub., Inc.*, 844 F.2d at 815. That case involved legislation that regulated waivers of the rule against newspaper-television cross-ownership in a way that targeted a single person “with the precision of a laser beam.” *Id.* at 814. The legislation, however, bore “only the most strained relationship to the purpose hypothesized by the [Government].” *Id.* Here, by contrast, the Act bears directly on the TikTok-specific national security harms identified and substantiated by the Government.

Moreover, as the Government notes, in certain respects TikTok received more process than would a company coming under the generally applicable provisions. TikTok participated in a prolonged negotiation with the Executive that featured numerous meetings and several proposals. It also received individualized consideration by the Congress prior to being required to divest. In contrast, under the generally applicable provisions the Executive need only provide “public notice” and issue a “public report” to the Congress prior to requiring a company to sever its ties to an adversary nation. § 2(g)(3)(B). In short, the Act singled out TikTok because of its known characteristics and history. It therefore did not violate TikTok’s constitutional right to equal protection of the laws.

#### **D. The Bill of Attainder Clause**

TikTok next claims the Act is a bill of attainder, and therefore prohibited by Article I, § 9, clause 3 of the Constitution. The Government responds that the Bill of Attainder Clause does not apply to corporations and that, in any event, the Act does not constitute a legislative punishment. We agree that the Act is not a bill of attainder.

A law is a bill of attainder if it “(1) applies with specificity, and (2) imposes punishment.” *BellSouth Corp. v. FCC (BellSouth II)*, 162 F.3d 678, 683 (D.C. Cir. 1998). Because the Act applies with specificity, this claim turns on whether the Act



can fairly be deemed a punishment. We conclude the Act is not a punishment under any of the three tests used to distinguish a permissible burden from an impermissible punishment.

Before turning to those tests, however, we briefly address the Government's threshold argument that the Bill of Attainder Clause does not apply to corporations. In other cases, we have assumed without deciding that the clause applies to corporations but emphasized that differences between commercial entities and persons need to be considered. *See, e.g., Kaspersky Lab, Inc. v. DHS*, 909 F.3d 446, 453–54, 461–63 (D.C. Cir. 2018) (assuming the Bill of Attainder Clause protects corporations but emphasizing the differences between corporations and “living, breathing human beings”); *BellSouth I*, 144 F.3d at 63 & n.5 (assuming the clause protects corporations but recognizing the importance of understanding “its effect on flesh-and-blood people”). We take the same approach here.

To determine whether a law constitutes a punishment, we analyze:

- (1) whether the challenged statute falls within the historical meaning of legislative punishment [the historical test];
- (2) whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes [the functional test]; and
- (3) whether the legislative record evinces a congressional intent to punish [the motivational test].

*Kaspersky Lab, Inc.*, 909 F.3d at 455 (cleaned up). The Act clearly is not a bill of attainder judged by any of these tests.

TikTok contends the Act satisfies the historical test because it bars TikTok from its chosen business. TikTok

reasons the prohibitions of the Act are close analogs to two categories of legislative action historically regarded as bills of attainder: confiscation of property and legislative bars to participation in a specific employment or profession. *See BellSouth II*, 162 F.3d at 685 (explaining the historical understanding of punishment). According to TikTok, the Act effectively requires TikTok to relinquish its property or see it rendered useless, and it precludes TikTok from continuing to participate in a legitimate business enterprise. As already explained, however, the Act requires a divestiture — that is, a sale, not a confiscation — as a condition of continuing to operate in the United States. *See BellSouth I*, 144 F.3d at 65 (explaining that although “structural separation is hardly costless, neither does it remotely approach the disabilities that have traditionally marked forbidden attainders”); *see also Kaspersky Lab, Inc.*, 909 F.3d at 462–63 (comparing a law requiring the Government to remove from its systems a Russia-based company’s software to the business regulations in the *BellSouth* cases). Nor is the divestiture requirement analogous to a legislative bar on someone’s participation in a specific employment or profession. *See Kaspersky Lab, Inc.*, 909 F.3d at 462 (rejecting a similar analogy in part “because human beings and corporate entities are so dissimilar” (cleaned up)).

The closer historical analog to the Act is a line-of-business restriction, which does not come within the historical meaning of a legislative punishment. *See BellSouth II*, 162 F.3d at 685 (observing “the Supreme Court has approved other line-of-business restrictions without ever suggesting that the restrictions constituted ‘punishment’” (collecting cases)); *Kaspersky Lab, Inc.*, 909 F.3d at 463 (explaining “the *BellSouth* cases make clear that the Bill of Attainder Clause tolerates statutes that, in pursuit of legitimate goals such as public safety or economic regulation, prevent companies from engaging in particular kinds of business or particular

combinations of business endeavors”). In fact, *BellSouth II* all but forecloses TikTok’s argument by recognizing that a “statute that leaves open perpetually the possibility of [overcoming a legislative restriction] does not fall within the historical meaning of forbidden legislative punishment.” 162 F.3d at 685 (quoting *Selective Serv. Sys. v. Minn. Pub. Int. Rsch. Grp.*, 468 U.S. 841, 853 (1984)) (brackets in original). The qualified divestiture exemption does just that. It “leaves open perpetually” the possibility of overcoming the prohibitions in the Act: TikTok can execute a divestiture and return to the U.S. market at any time without running afoul of the law.

The Act also passes muster under the functional test. For purposes of this analysis, the “question is not whether a burden is proportionate to the objective, but rather whether the burden is so disproportionate that it belies any purported nonpunitive goals.” *Kaspersky Lab, Inc.*, 909 F.3d at 455 (cleaned up). Considering our conclusion that the Act passes heightened scrutiny for purposes of the First Amendment, it obviously satisfies the functional inquiry here: The Act furthers the Government’s nonpunitive objective of limiting the PRC’s ability to threaten U.S. national security through data collection and covert manipulation of information. The Government’s solution to those threats “has the earmarks of a rather conventional response to a security risk: remove the risk.” *Id.* at 457 (cleaned up). In other words, the Government’s attempt to address the risks posed by TikTok reflects a forward-looking prophylactic, not a backward-looking punitive, purpose. That is sufficient to satisfy the functional analysis. *See id.* at 460 (stating the functional test “does not require that the Congress precisely calibrate the burdens it imposes to the goals it seeks to further or to the threats it seeks to mitigate” (cleaned up)).

The so-called motivational test, for its part, hardly merits discussion. “Given the obvious restraints on the usefulness of

legislative history,” congressional intent to punish is difficult to establish. *Id.* at 463 (cleaned up); *see also BellSouth II*, 162 F.3d at 690 (“Several isolated statements are not sufficient to evince punitive intent” (cleaned up)). Indeed, the motivational test is not “determinative in the absence of unmistakable evidence of punitive intent.” *Id.* (cleaned up). TikTok does not come close to satisfying that requirement. We therefore conclude the Act does not violate the Bill of Attainder Clause under any of the relevant tests.

#### **E. The Takings Clause**

TikTok claims the Act constitutes a per se regulatory taking in violation of the Fifth Amendment because it will render TikTok defunct in the United States. The Government counters that TikTok has assets that can be sold, and that the Act requires only divestiture, which need not be uncompensated. Although the Act will certainly have a substantial effect on the TikTok platform in the United States, regardless whether TikTok divests, the Act does not qualify as a per se regulatory taking.

The Supreme Court recognizes two situations in which regulatory action constitutes a per se taking: (1) where the government requires that an owner suffer a “physical invasion of [its] property,” and (2) where a regulation “completely deprives an owner of *all* economically beneficial use of [its] property.” *Lingle v. Chevron U.S.A. Inc.*, 544 U.S. 528, 538 (2005) (cleaned up); *see Cedar Point Nursery v. Hassid*, 594 U.S. 139, 153 (2021) (explaining the first category includes temporary invasions of property). TikTok’s argument is of the second variety, but it does not demonstrate the complete deprivation such a claim requires.

Here the causal connection between the Act and the alleged diminution of value is attenuated because the Act

authorizes a qualified divestiture before (or after) any prohibitions take effect. That presents TikTok with a number of possibilities short of total economic deprivation. ByteDance might spin off its global TikTok business, for instance, or it might sell a U.S. subset of the business to a qualified buyer.

TikTok dismisses divestiture as impractical. One of the main impediments, however, appears to be export prohibitions that the PRC erected to make a forced divestiture more difficult if not impossible. But the PRC, not the divestiture off-ramp in the Act, is the source of TikTok's difficulty. TikTok would have us turn the Takings Clause into a means by which a foreign adversary nation may render unconstitutional legislation designed to counter the national security threats presented by that very nation.

In any event, TikTok has not been subjected to a complete deprivation of economic value. Beyond characterizing divestiture as impossible, TikTok does not dispute that it has assets that can be sold apart from the recommendation engine, including its codebase; large user base, brand value, and goodwill; and property owned by TikTok. In other words, TikTok has several economically beneficial options notwithstanding the PRC's export restriction.

#### **F. Alternative Relief**

As an alternative to permanently enjoining the Act, the petitioners suggest we issue a temporary injunction and appoint a special master to make procedural recommendations or recommend factual findings. Because we have now resolved the case on the merits, we deny these requests as moot. The petitioners further object to the Government having filed classified material and releasing to them only a redacted version. Our decision, however, rests solely on the unredacted, public filings in this case. *See China Telecom (Ams.) Corp.*,

57 F.4th at 264 (similarly relying on an unclassified record). Notwithstanding the significant effect the Act may have on the viability of the TikTok platform, we conclude the Act is valid based upon the public record.<sup>11</sup>

### III. Conclusion

We recognize that this decision has significant implications for TikTok and its users. Unless TikTok executes a qualified divestiture by January 19, 2025 — or the President grants a 90-day extension based upon progress towards a qualified divestiture, § 2(a)(3) — its platform will effectively be unavailable in the United States, at least for a time. Consequently, TikTok’s millions of users will need to find alternative media of communication. That burden is attributable to the PRC’s hybrid commercial threat to U.S. national security, not to the U.S. Government, which engaged with TikTok through a multi-year process in an effort to find an alternative solution.

The First Amendment exists to protect free speech in the United States. Here the Government acted solely to protect that freedom from a foreign adversary nation and to limit that adversary’s ability to gather data on people in the United States.

For these reasons the petitions are,

*Denied.*

---

<sup>11</sup> Accordingly, we grant the Government’s motion for leave to file classified materials and direct the Clerk to file the lodged materials, though we do not rely on them in denying the petitions.

SRINIVASAN, *Chief Judge*, concurring in part and concurring in the judgment:

I fully join all aspects of the court's opinion today other than Part II.B, which rejects TikTok's First Amendment challenge. As to that challenge, I agree with my colleagues that the Act does not violate the First Amendment. But I reach that conclusion via an alternate path. My colleagues do not decide whether the Act should be subjected to the strictest First Amendment scrutiny or instead the lesser standard of intermediate scrutiny because, in their view, the Act satisfies strict scrutiny regardless. I see no need to decide whether the Act can survive strict scrutiny, because, in my view, the Act need only satisfy intermediate scrutiny, which it does. I would thus answer the question my colleagues leave open while leaving open the question they answer.

Two features of the Act support applying intermediate rather than strict scrutiny to resolve TikTok's First Amendment challenge. First, in step with longstanding restrictions on foreign control of mass communications channels, the activity centrally addressed by the Act's divestment mandate is that of a foreign nation rather than a domestic speaker—indeed, not just a foreign nation but a designated foreign adversary. Second, the Act mandates divestment of that foreign adversary's control over TikTok for reasons lying outside the First Amendment's heartland: one reason that is wholly unrelated to speech, and another that, while connected to speech, does not target communication of any specific message, viewpoint, or content.

In those circumstances, the Act's divestment mandate need not be the least restrictive means of achieving its national-security objectives, as strict scrutiny would require. Rather, it is enough if, per intermediate scrutiny, the divestment mandate is not substantially broader than necessary to meet those goals. The Act meets that standard.

2

A.

TikTok’s First Amendment challenge “implicates the gravest and most delicate duty that courts are called on to perform: invalidation of an Act of Congress.” *Hodge v. Talkin*, 799 F.3d 1145, 1157 (D.C. Cir. 2015) (formatting modified) (quoting *Blodgett v. Holden*, 275 U.S. 142, 147–48 (1927) (Holmes, J., concurring)). And that “most delicate duty” presents itself here in a setting in which courts already proceed with suitable caution—when called upon to review the political branches’ judgments about national security. A strong bipartisan majority of both Houses of Congress, together with two successive Presidents (one of whom is also the President-elect), have determined that divesting TikTok from PRC control is a national-security imperative. *See Op., ante*, at pp. 11–16.

While that is the political branches’ across-the-board assessment of a pressing national-security issue today, we also take stock of history when considering whether their response stays within the bounds of the First Amendment. An established “history and tradition of regulation [is] relevant when considering the scope of the First Amendment.” *City of Austin v. Reagan Nat’l Advert. of Austin, LLC*, 596 U.S. 61, 75 (2022) (citing *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 446 (2015)); *see Vidal v. Elster*, 602 U.S. 286, 301 (2024). It goes without saying that a social media app through which some 170 million Americans absorb information and engage with each other and the world—in the palm of their hands—is a recent phenomenon. But concerns about the prospect of foreign control over mass communications channels in the United States are of age-old vintage. In that respect, Congress’s decision to condition TikTok’s continued operation in the United States on severing Chinese control is not a historical outlier. Rather, it is in line with a historical pattern.



The first communications medium capable of reaching mass audiences in real time—radio—was subject to restrictions on foreign ownership and control from the very outset. The Radio Act of 1912 required radio operators engaged in interstate (or international) communications to obtain a license from the Secretary of Commerce and Labor, but Congress made licenses available only to U.S. citizens or companies. Pub. L. No. 62-264, §§ 1–2, 37 Stat. 302, 302–03 (repealed 1927). Congress then extended the restrictions to encompass foreign control (not just foreign ownership) in the Radio Act of 1927, prohibiting licensing of any company if it had a foreign officer or director or if one-fifth of its capital stock was in foreign hands. Pub. L. No. 69-632, § 12, 44 Stat. 1162, 1167 (repealed 1934).

Within a few years, the Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064, shored up the restrictions on foreign control. Section 310 of the law incorporated with little change the 1927 Act’s foreign-control requirements, and also gave the newly created Federal Communications Commission (FCC) authority to withhold a license if a company is “directly or *indirectly* controlled” by a foreign-dominated parent company. *Id.* § 310(a), 48 Stat. at 1086 (emphasis added) (today codified at 47 U.S.C. § 310(b)(4) (2024)). In urging Congress to adopt the additional restrictions on foreign control, the Navy conveyed its concerns that foreign-controlled stations could “be employed in espionage work and in the dissemination of subversive propaganda.” Hearings on H.R. 8301 Before the H. Comm. on Interstate & Foreign Com., 73d Cong. 26 (1934). The FCC has described Section 310’s original purpose as “protect[ing] the integrity of ship-to-shore and governmental communications” from foreign interference and “thwart[ing] the airing of foreign propaganda on broadcast stations.” Foreign Investment in Broadcast Licenses, 78 Fed. Reg. 75563, 75564 (Nov. 13, 2013).

Section 310 continues to restrict foreign control of radio licenses, including ones used for broadcast communication and wireless cellular services. *See* 47 U.S.C. § 310(a)–(b). And while that provision regulates wireless licenses, limitations on foreign control also exist for *wired* transmission lines under Section 214 of the same law. 47 U.S.C. § 214(a); *see also id.* § 153(11), (50)–(53).

When deciding whether to issue or revoke a Section 214 authorization, the FCC considers “the public convenience and necessity,” *id.* § 214(c), including the implications for “national defense,” *id.* § 151. In conducting that inquiry, the FCC assesses whether direct or indirect foreign ownership or control of a transmission line raises national-security or foreign-policy concerns. *See Rules & Policies on Foreign Participation in the U.S. Telecomm. Mkt.*, 12 FCC Rcd. 23891, 23918–21 (1997). The FCC consults with Executive Branch agencies “to help assess national security and other concerns that might arise from a carrier’s foreign ownership.” *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 261 (D.C. Cir. 2022). Those “Executive Branch agencies may review existing authorizations for national-security risks and recommend revocation if the risks cannot be mitigated.” *Id.* at 262.

Notably, the FCC in recent years has exercised its Section 214 authority to deny or revoke transmission authorizations in the case of U.S. entities subject to ultimate Chinese control. The Commission’s rationale has mirrored Congress’s motivation for the Act we consider in this case—i.e., national-security concerns that the PRC could leverage its control over foreign parent companies to require U.S. subsidiaries to provide China with access to U.S. communications lines, thereby enabling espionage and other harmful undertakings. *See Pac. Networks Corp. & ComNet (USA) LLC*, 37 FCC Rcd. 4220 (2022); *China Telecom (Americas) Corp.*, 36 FCC Rcd.

15966 (2021); *China Mobile Int'l (USA)*, 34 FCC Rcd. 3361 (2019). This court has affirmed those FCC decisions. *See Pac. Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023); *China Telecom*, 57 F.4th 256.

*China Telecom*, for example, involved a U.S. company with a Section 214 authorization whose parent corporation was majority-owned by a Chinese governmental entity. *See* 57 F.4th at 260, 265. The FCC's revocation of China Telecom's authorization was "grounded [in] its conclusion that China Telecom poses an unacceptable security risk" because "the Chinese government is able to exert significant influence over [it]." *Id.* at 265. In rejecting China Telecom's claim that the asserted national-security risk was unduly speculative, we noted that Chinese law obligates Chinese companies "to cooperate with state-directed cybersecurity supervision and inspection," and we cited "compelling evidence that the Chinese government may use Chinese information technology firms as vectors of espionage and sabotage." *Id.* at 265–66. We additionally explained that "[i]n the national security context," the FCC "need not wait for a risk to materialize before revoking a section 214 authorization." *Id.* at 266.

*China Telecom* is a present-day application of the kinds of restrictions on foreign control that have existed in the communications arena since the dawn of radio. That longstanding regulatory history bears on the First Amendment analysis here. *See City of Austin*, 596 U.S. at 75. That is so even though some of that history arose in the context of broadcast, a medium in which the Supreme Court has "recognized special justifications for regulation." *Reno v. Am. Civ. Liberties Union*, 521 U.S. 844, 868 (1997). Some of the relevant history also arose outside of broadcast (e.g., authorizations for wired transmission lines under Section 214), and certain regulatory concerns are present to a far greater

degree with modern communications media than with traditional broadcast (e.g., the vastly enhanced potential for collection of data from and about users).

To be sure, because communications media reaching mass audiences in real time “were not present in the founding era,” the regulatory history naturally does not date back that far. *See City of Austin*, 596 U.S. at 75. But under the Supreme Court’s decisions, regulatory history still matters so long as the relevant kind of “regulation followed” on the heels of the emergence of a new type of communication medium. *Id.* In fact, it can matter for precisely the issue considered here: whether a First Amendment challenge should be examined under strict or intermediate scrutiny.

So, in *City of Austin*, the Supreme Court recently assessed which of those standards should govern a challenge to a law attaching different restrictions to off-premises and on-premises signage. *See id.* at 67–69. The Court explained that comparable regulations emerged relatively soon after outdoor billboards first appeared in the 1800s. *See id.* at 65–66, 75. To the Court, that “unbroken tradition of on-/off-premises distinctions counsel[ed] against” subjecting the challenged law to strict scrutiny. *Id.* at 75. If so there, so too here.

## B.

In *City of Austin*, the Supreme Court considered the longstanding regulatory history as part of its inquiry into whether the law in question should be deemed content based or content neutral. *See* 596 U.S. at 69–76. That distinction in turn informs the standard of scrutiny. Under hornbook First Amendment doctrine, content-based laws generally pose more pronounced First Amendment concerns and so usually must satisfy strict scrutiny. *See Reed v. Town of Gilbert*, 576 U.S. 155, 163–64 (2015); *cf. City of Austin*, 596 U.S. at 73 (noting

that regulation of commercial speech has been subject to intermediate scrutiny even when content based). Content-neutral laws, on the other hand, present less substantial First Amendment concerns and so generally trigger, at most, intermediate scrutiny. *See Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994) (*Turner I*).

There can also be, though, an antecedent question: whether the First Amendment applies at all. The question arises here because the effect of the Act's divestment mandate falls most directly on foreign entities: the Act targets the PRC, a foreign sovereign, and the divestment mechanism established by Congress necessarily encompasses ByteDance, a foreign company subject to the PRC's control. That recognition brings into play the settled understanding that "foreign organizations operating abroad have no First Amendment rights." *Agency for Int'l Dev. v. All. for Open Soc'y Int'l Inc.*, 591 U.S. 430, 436 (2020).

The Act requires TikTok to divest the corporate parent, ByteDance, because ByteDance is subject to the PRC's control. ByteDance developed and maintains the source code underlying TikTok's recommendation engine, *see* Simkins Decl. ¶¶ 52, 57, 90 (TikTok App. 738, 740, 751); Presser Decl. ¶¶ 63–64 (TikTok App. 832), so the company has the ability to curate the content sent to TikTok users. That kind of curation function, when the First Amendment applies, is protected expressive activity. As the Supreme Court recently explained, "presenting a curated compilation of speech originally created by others" via a social media app is a form of expression. *Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2400 (2024); *see id.* at 2400–02. So, by forcing ByteDance to split from TikTok, the Act abolishes the ability of ByteDance—and ultimately the PRC, Congress's true concern—to curate content going to TikTok's U.S. users.

To the extent the PRC or ByteDance might wish to adjust the content viewed by U.S. users of TikTok, those curation decisions would be made abroad. *See* Milch Decl. ¶ 29 (TikTok App. 661) (explaining that TikTok’s proposed security measures contemplate “continued reliance on ByteDance engineers for . . . its recommendation engine”). The PRC and ByteDance thus would lack any First Amendment rights in connection with any such curation actions. *Agency for Int’l Dev.*, 591 U.S. at 436. That is true even though the PRC or ByteDance, in that scenario, would aim their curation decisions at the United States. The Supreme Court’s decision in *Agency for International Development* demonstrates the point.

That case involved foreign organizations’ speech that was targeted in part at the United States, yet the Court still applied the rule that the foreign speakers lack any First Amendment rights when engaged in expressive activity abroad. The federal statute challenged in *Agency for International Development* required organizations receiving certain U.S. aid dollars to espouse a policy opposing prostitution. *Id.* at 432. The Court first held that the compelled adoption of an anti-prostitution viewpoint violated the First Amendment as applied to U.S. funding recipients. *See Agency for Int’l Dev. v. All. for Open Soc’y Int’l Inc.*, 570 U.S. 205, 214 (2013). But the Court later rejected a parallel challenge brought by foreign funding recipients, reasoning that foreign organizations lack any First Amendment rights in connection with their expressive activities abroad. *Agency for Int’l Dev.*, 591 U.S. at 433–36. And that was so even though the relevant speech act—the mandated expression of opposition to prostitution—was aimed in part at the United States: in fact, the way the funding recipients demonstrated adherence to the funding condition was to express opposition to prostitution in the “award

9

documents” exchanged with the U.S. Agency for International Development. *See Agency for Int’l Dev*, 570 U.S. at 210.

In short, while the Act’s divestment mandate directly affects—and aims to eliminate—the ability of the PRC and ByteDance to engage with U.S. users of a PRC-controlled TikTok, it raises no First Amendment concerns vis-à-vis those foreign actors.

C.

Even if ByteDance and the PRC lack First Amendment rights to assert against the Act’s divestment mandate, what about the U.S.-based petitioners’ free-speech claims? The principal U.S. petitioners are: (i) TikTok Inc., the U.S. subsidiary of ByteDance that provides the TikTok platform in the United States; and (ii) U.S. TikTok users, who are both creators and viewers of TikTok content.

1.

For TikTok Inc., the Act is designed to sever ByteDance from the platform but leave untouched TikTok Inc.’s expression on a post-divestment version of the app. TikTok Inc. both creates and curates content on the platform, and the Act does not restrict those speech and curation choices. TikTok Inc. posts videos to its own TikTok account and would remain fully free to continue doing so post-divestment. The company can also engage in content moderation, including through enforcement of community guidelines that excise videos containing nudity, for instance. *See Op., ante*, at p. 27. To the extent those choices are TikTok Inc.’s own, the company could maintain the same editorial policies on a post-divestment version of the app.

10

TikTok also claims that TikTok Inc.’s deployment of the platform’s recommendation engine in the U.S. is itself an expressive decision. Even assuming so, after divestment, a non-Chinese-controlled TikTok could still use the same algorithm to promote the same exact mix of content presently appearing on the app. According to TikTok, however, Chinese law would prevent the export of the algorithm fueling the recommendation engine without the PRC’s approval, which it would not grant. TikTok Br. 24. The *Act*, though, would not dictate that outcome. Rather, the PRC, backed by Chinese law, would. And Congress of course need not legislate around another country’s preferences to exercise its own powers constitutionally—much less the preferences of a designated foreign adversary, the very adversary whom Congress determined poses the fundamental threat to national security prompting the *Act* in the first place.

2.

The last group of petitioners bringing a First Amendment claim are users who create and consume content on the TikTok platform. They face the prospect of the app becoming unavailable to them if a divestment does not occur within the window allowed by Congress, or of an app potentially altered in certain ways if a divestment were to take place.

A threshold question bearing significantly on the assessment of their First Amendment challenge is which standard of scrutiny should apply: strict or intermediate scrutiny. The choice can be an important, potentially outcome-determinative one, which is why the Supreme Court can devote entire decisions to the issue. *See, e.g., City of Austin*, 596 U.S. 61. That choice here, as is often the case, turns in significant measure on the rationale for the challenged law, which informs whether the law is considered content based or content neutral.



As my colleagues explain, the Act's divestment mandate rests on two justifications, both of which concern the PRC's ability (through its control over ByteDance) to exploit the TikTok platform in ways inimical to U.S. national security. *See Op.*, ante, at p. 33. First, the PRC could harvest abundant amounts of information about the 170 million U.S. app users and potentially even their contacts. Second, the PRC could direct the TikTok platform to covertly manipulate the content flowing to U.S. users. To the government, a foreign adversary's ability to acquire sensitive information on Americans and secretly shape the content fed to Americans would pose a substantial threat to U.S. national security.

Those dual interests are manifested in the terms of the Act, in its central provisions establishing the divestment requirement. The Act defines a "qualified divestiture" as one that removes any ongoing relationship with the foreign adversary-controlled entities with which the app was previously affiliated, including in particular "any cooperation with respect to *the operation of a content recommendation algorithm* or an agreement with respect to *data sharing*." § 2(g)(6)(B) (emphasis added). In the central operative provision of the Act, then, Congress established that a divestiture must satisfy the two national-security concerns invoked by the government in this case: data protection and content manipulation.

An examination of those interests, separately and in combination, shows that the Act does not raise the kinds of core free-speech concerns warranting the application of strict scrutiny. Instead, intermediate scrutiny should apply.

12

a.

The data-protection rationale is plainly content neutral, supporting the application of intermediate rather than strict scrutiny. There is no sense in which the data-protection interest relates to the content of speech appearing on TikTok. In fact, the interest does not relate to speech at all, raising the question whether it would even trigger intermediate scrutiny if it stood alone.

In *Arcara v. Cloud Books, Inc.*, 478 U.S. 697 (1986), for instance, the Supreme Court considered a First Amendment challenge to the proposed closure of a bookstore because prostitution took place there. The Court declined to apply even intermediate scrutiny. The Court explained that, while the First Amendment claim arose from the establishment's engagement in the protected activity of selling books, that activity had nothing to do with the reasons for the proposed closure. *See id.* at 705. The Court analogized the circumstances to ones in which a "city impose[s] closure penalties for demonstrated Fire Code violations or health hazards from inadequate sewage treatment." *Id.* In such a situation, "the First Amendment would not aid the owner of premises who had knowingly allowed such violations to persist." *Id.*

Here, similarly, the data-protection rationale has nothing to do with the expressive activity taking place on the TikTok platform. Any enterprise collecting vast amounts of data from users, whatever its line of business, could pose that sort of risk. That is not to diminish the burdens on millions of U.S. users if the TikTok platform were to become unavailable to them as a forum for expressive activity. All of them could be faced with needing to find an alternate venue. The same was true, though, of the bookstore patrons in *Arcara*, yet the Court still denied

the First Amendment challenge to the bookstore's closure without even applying intermediate scrutiny.

To be sure, the *Arcara* Court observed that First Amendment scrutiny would apply to a law that “inevitably single[s] out bookstores or others engaged in First Amendment protected activities for the imposition of its burden.” *Id.* Even if that description has salience here—which is not at all clear—the Court has explained that such a law may be “justified by some special characteristic” of the regulated entities. *Minneapolis Star v. Minn. Comm’r of Rev.*, 460 U.S. 575, 585 (1983); *Turner I*, 512 U.S. at 660–61. The vast data-collection practices of TikTok and similar applications subject to the Act would seem to qualify as just such a “special characteristic.”

At any rate, there is no need to reach a firm conclusion on whether the data-protection interest, if considered in isolation, would trigger the application of intermediate scrutiny or instead an even more relaxed form of review. That is because the government makes no argument that the Act's application to TikTok should be sustained based on the data-protection interest alone. It is necessary, then, to engage with the other interest underpinning the Act, to which I turn next.

b.

Congress's interest in preventing the PRC's use of TikTok to engage in covert content manipulation is self-evidently connected to speech: it centers on the potential reactions of American viewers to covert content-curation decisions made by the PRC. Still, that interest does not raise heartland First Amendment concerns about content-based restrictions for reasons I will explain—so much so that, even if that interest were the sole rationale for the Act, there would still be a strong argument for applying intermediate rather than strict scrutiny.

It is important to keep in mind, though, that Congress's covert-content-manipulation concern does not stand alone. There is also its distinct data-protection interest that supports applying (at most) intermediate scrutiny, along with the consistent regulatory history of restricting foreign control of mass communications channels that likewise weighs in favor of intermediate scrutiny. So, the question ultimately is not whether the covert-content-manipulation concern itself would occasion applying strict scrutiny, but rather whether it so strongly and clearly does that it overcomes the other important considerations counseling *against* strict scrutiny. I believe it does not.

First, even assuming the covert-content-manipulation concern may bear the indicia of a content-based rationale, it would do so only marginally. The Supreme Court has used slightly varying formulations when describing what makes a law content based, but this recent articulation captures the gist: not just “*any* examination of speech or expression inherently” makes a regulation content based; rather, “it is regulations that discriminate based on ‘the topic discussed or the idea or message expressed’ that are content based.” *City of Austin*, 596 U.S. at 73–74 (quoting *Reed*, 576 U.S. at 171); *see Op.*, *ante*, at p. 28.

Congress's concern about the PRC's capacity to conduct covert content manipulation on the TikTok platform does not “discriminate based on the topic discussed or the idea or message expressed.” *City of Austin*, 596 U.S. at 73–74 (internal quotation marks omitted). Congress desires to prevent the PRC's secret curation of content flowing to U.S. users *regardless* of the topic, idea, or message conveyed. *See* Gov't Br. 66–68. To be sure, Congress would have concerns about the PRC covertly compelling ByteDance to flood the feeds of American users with pro-China propaganda. But

Congress would also have concerns about the PRC sowing discord in the United States by promoting videos—perhaps even primarily truthful ones—about a hot-button issue having nothing to do with China. Indeed, because the concern is with the PRC’s manipulation of the app to advance China’s *interests*—not China’s views—one can imagine situations in which it would even serve the PRC’s interests to augment *anti-China, pro-U.S.* content. Suppose, for instance, the PRC determines that it is in its interest to stir an impression of elevated anti-China sentiment coming from the United States—say, to conjure a justification for actions China would like to take against the United States. That would qualify as covert content manipulation of the kind that concerned Congress and supports the Act’s divestment mandate.

Congress’s concern with covert content manipulation by a foreign adversary in any direction and on any topic—rather than on particular messages, subjects, or views—is evident in the Act’s terms and design. See *City of Renton v. Playtime Theaters, Inc.*, 475 U.S. 41, 48 (1986); *Turner I*, 512 U.S. at 646–49, 652. Recall that the Act asks whether there is the prospect of “any cooperation” with an entity controlled by a foreign adversary “with respect to the operation of a content recommendation algorithm.” § 2(g)(6)(B). The concern is a general one about control of a “content recommendation algorithm,” without regard to whether the content choices enabled by that control might point in a specific direction or involve a specific matter.

As is reflected in the title of the Act—“Protecting Americans From Foreign Adversary Controlled Applications Act”—Congress aimed not to address specific content but to address specific actors: in particular, to prevent a “foreign adversary” from exercising control over covered applications. In that sense, the law operates in the nature of a speaker-based

restriction. As applied here, what matters is whether a particular potential curator, the PRC, has the ability to control (covertly) the content fed to TikTok's U.S. users, regardless of what the content may be. True, "laws favoring some speakers over others demand strict scrutiny" when the "speaker preference reflects a content preference." *Reed*, 576 U.S. at 171 (quoting *Turner I*, 512 U.S. at 658). But here, the speaker (non)preference is not grounded in a content preference.

In certain respects, in fact, the Act resembles a time, place, or manner regulation—a type of regulation generally subject to intermediate scrutiny. *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984); *Ward v. Rock Against Racism*, 491 U.S. 781, 791, 798–99 (1989). The Act restricts only one way in which the Chinese government can project information into the United States—the covert manipulation of content on TikTok. The Act does not touch on the PRC's ability to communicate through any medium other than TikTok (and potentially other "covered" applications, *see* § 2(g)(2)(A)). Indeed, as far as the Act is concerned, the PRC would be free to publish its own videos—whether labeled as such or camouflaged as cutout accounts—on a post-divestment version of *TikTok itself*. So understood, the Act does not prevent Americans from receiving any message from the PRC; it only prevents the PRC from secretly manipulating the content on a specific channel of communication that it ultimately controls.

Those circumstances are far removed from *Lamont v. Postmaster General*, 381 U.S. 301 (1965), on which petitioners heavily rely. *Lamont* concerned a law requiring anyone in the United States who desired to receive mail deemed by the Secretary of the Treasury to be "communist political propaganda" to affirmatively notify the Postal Service. *Id.* at 302–03. The Supreme Court invalidated the statute, resting its

decision “on the narrow ground that the addressee in order to receive his mail must request in writing that it be delivered.” *Id.* at 307. That obligation amounted to “an unconstitutional abridgement of the addressee’s First Amendment rights,” because “any addressee is likely to feel some inhibition in sending for literature which federal officials have condemned as ‘communist political propaganda.’” *Id.*

This case does not involve the “narrow ground” on which the Court rooted its decision in *Lamont*: an affirmative obligation to out oneself to the government in order to receive communications from a foreign country that are otherwise permitted to be here. Moreover, whereas this case, as explained, addresses what amounts to a speaker-based regulation without a content preference underpinning it, the law in *Lamont* drew a viewpoint-based distinction based on whether the government deemed mailed material “communist political propaganda.” Finally, *Lamont* was not a case about *covert* content manipulation, the concern driving the Act’s divestment mandate. In that regard, while counterspeech is an available response in the case of a publication designated as “communist political propaganda,” counterspeech is elusive in response to covert (and thus presumably undetected) manipulation of a social media platform.

\* \* \*

For all those reasons, Congress’s concern with the PRC’s potential exercise of covert content manipulation should not give rise to strict scrutiny. That concern does not bear the hallmarks of a content-based rationale; the Act’s other justification concerning data protection is plainly a content-neutral one; and there has been a long regulatory history of restrictions on foreign control of mass communications channels.

18

D.

To satisfy intermediate scrutiny, a law needs to meet two requirements: (i) the law must further “important” (or “substantial” or “legitimate”) governmental interests; and (ii) the means must be narrowly tailored to serve those interests. *See Turner I*, 512 U.S. at 661–62; *Ward*, 491 U.S. at 791, 796, 798–99. Under strict scrutiny, by comparison: (i) the governmental interests must be “compelling”; and (ii) the means must be the least-restrictive way of serving them. *E.g.*, *McCullen v. Coakley*, 573 U.S. 464, 478 (2014). As to the second prong, the Supreme Court has explained that the “narrow tailoring” test under intermediate scrutiny requires less than the least-restrictive-means test under strict scrutiny, with the former met “[s]o long as the means chosen are not substantially broader than necessary to achieve the government’s interest.” *Ward*, 491 U.S. at 800.

Here, the Act satisfies both prongs of the intermediate scrutiny test.

1.

Recall that, as manifested in the Act’s terms and design, *see* § 2(g)(6)(B), Congress mandated TikTok’s divestment in order to prevent the PRC from capturing the personal data of millions of Americans and surreptitiously manipulating the content the app serves them. Each of those objectives qualifies as an important governmental interest.

a.

The data-protection interest aims to protect U.S. national security by depriving the PRC of access to a vast dataset of granular information on 170 million Americans. Congress’s interest is important and well grounded.



As TikTok does not dispute, the platform collects vast amounts of information from and about its American users. *See* TikTok App. 820; Privacy Policy, TikTok (Aug. 28, 2024), <https://perma.cc/XE6G-F86Q>. The government’s national-security concerns about the PRC’s access to that data take two forms. First, the PRC could exploit sensitive data on individual Americans to undermine U.S. interests, including by recruiting assets, identifying Americans involved in intelligence, and pressuring and blackmailing our citizens to assist China. Second, the vast information about Americans collected by TikTok amounts to the type of “bulk” dataset that could “greatly enhance” China’s development and use of “artificial intelligence capabilities.” Vorndran Decl. ¶ 32 (Gov’t App. 37).

Those national-security concerns self-evidently qualify as important. To be sure, the fears must be “real, not merely conjectural.” *Turner I*, 512 U.S. at 664. And petitioners submit that the government’s concerns about the PRC accessing user data from the TikTok platform are unduly speculative and insufficiently grounded. I cannot agree.

When applying intermediate scrutiny, a court “must accord substantial deference to the predictive judgments of Congress,” and “[o]ur sole obligation is to assure that, in formulating its judgments, Congress has drawn reasonable inferences based on substantial evidence.” *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 195 (1997) (*Turner II*) (internal quotation marks omitted). That bar is cleared here.

In evaluating whether Congress’s national-security concerns are adequately grounded, we can take stock of the Executive Branch’s elaborations as submitted in declarations. *See Humanitarian Law Project*, 561 U.S. at 33. As my colleagues set out, *Op.*, *ante*, at pp. 34–36, and as the

government explains, Congress’s data-security concern arises against a backdrop of broadscale “overt and covert actions” by the PRC “to undermine U.S. interests,” Blackburn Decl. ¶ 23 (Gov’t App. 8). Collecting data on Americans is a key part of that multi-faceted strategy. *See id.* ¶¶ 31–33 (Gov’t App. 10–11). The PRC has engaged in extensive efforts to amass data on Americans for potential use against U.S. interests. *Id.* ¶ 31 (Gov’t App. 10–11). And the PRC “is rapidly expanding and improving its artificial intelligence and data analytics capabilities for intelligence purposes,” enabling it to exploit access to large datasets in increasingly concerning ways. *Id.* ¶ 30 (Gov’t App. 10).

“ByteDance and TikTok present powerful platforms” for those purposes. *Id.* ¶ 36 (Gov’t App. 13). It is a modus operandi of the PRC to surreptitiously access data through its control over companies like ByteDance. While the PRC has sometimes obtained data through aggressive hacking operations, it also attempts to do so by “leverag[ing] access through its relationships with Chinese companies.” *Id.* ¶ 33 (Gov’t App. 11). Even if the PRC has yet to discernibly act on its potential control over ByteDance’s access to data on American users in particular, Congress did not need to wait for the risk to become realized and the damage to be done before taking action to avert it. *See Humanitarian Law Project*, 561 U.S. at 34–35; *China Telecom*, 57 F.4th at 266–67. That is particularly so in light of the PRC’s broader, long-term geopolitical strategy of pre-positioning assets for potential use against U.S. interests at pivotal moments. *See Vorndran Decl.* ¶ 12 (Gov’t App. 34); Blackburn Decl. ¶ 26 (Gov’t App. 9).

In these circumstances, in short, Congress’s data-protection concern is hardly speculative or inadequately grounded in this murky corner of national security.

21

b.

The same is true of Congress's concern about the PRC's covert content manipulation. Our duty to accord deference to Congress's determinations when applying intermediate scrutiny, *Turner II*, 520 U.S. at 195, is all the more important in the area of national security. Like its data-protection concern, Congress's content-manipulation concern "arise[s] in connection with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess." *Humanitarian Law Project*, 561 U.S. at 34. In matters of national security, Congress must often rely on its—and the Executive Branch's—"informed judgment rather than concrete evidence." *Id.* at 34–35. And "[t]hat reality affects what we may reasonably insist on from the Government." *Id.* at 35. The government's "evaluation of the facts" is "entitled to deference." *Id.* at 33.

As the government details and petitioners do not dispute, the PRC engages in an aggressive, global campaign of influence operations against U.S. interests, relying heavily on the internet and social-media platforms. Blackburn Decl. ¶¶ 28–29 (Gov't App. 9–10). Across the globe, the PRC seeks to "promote PRC narratives . . . and counter other countries' policies that threaten the PRC's interests." *Id.* ¶ 29 (Gov't App. 10). That includes increasingly pronounced efforts to "mold" America's "public discourse" and "magnify" our "societal divisions." *Id.*

It was reasonable for Congress to infer from the information available to it that, if directed by the PRC to assist in those efforts, ByteDance and TikTok "would try to comply." *Id.* ¶ 69 (Gov't App. 23). The government points to examples of when "the PRC has exerted control over the content shown on other ByteDance-managed apps." Vorndran Decl. ¶ 33

(Gov't App. 38). And were the PRC to exert that kind of covert control over the content on TikTok, it would be “difficult—if not impossible—to detect, both by TikTok users and by law enforcement personnel.” *Id.* ¶ 34 (Gov't App. 38). In that context, Congress's concern with preventing the PRC's covert content manipulation of the platform readily qualifies as an important, well-founded governmental interest.

In resisting that conclusion, petitioners contend that the covert-content-manipulation rationale cannot be an important governmental interest because it is “related to the suppression of free expression.” *NetChoice*, 144 S. Ct. at 2407. Petitioners are mistaken.

As an initial matter, insofar as petitioners believe that a law can *never* satisfy First Amendment scrutiny if it is “related to the suppression of free expression,” that is incorrect. The consequence of a law's being deemed “related to the suppression of expression” is not that the law is then per se invalid, but instead that it is then subject to strict rather than intermediate scrutiny. *See Humanitarian Law Project*, 561 U.S. at 28 (citing *Texas v. Johnson*, 491 U.S. 397, 403 (1989)). In this case, for all the reasons previously explained, the Act's divestment mandate is more appropriately assessed under intermediate scrutiny than strict scrutiny.

That conclusion is fully consistent with *NetChoice*, as the laws at issue there were “related to the suppression of expression” in a way untrue of the Act. In *NetChoice*, two states enacted laws addressing perceived bias against conservative viewpoints on large social-media platforms like YouTube and Facebook. 144 S. Ct. at 2394. The laws restricted the platforms' ability to remove, label, or deprioritize posts or users based on content or viewpoint. *Id.* at 2395–96. The laws did so, the Supreme Court explained, in pursuit of an

objective “to correct the mix of speech that the major social-media platforms present,” so as “to advance [the states’] own vision of ideological balance.” *Id.* at 2407. The Court explained that such an interest “is very much related to the suppression of free expression, and it is not valid, let alone substantial.” *Id.* (citing *Buckley v. Valeo*, 424 U.S. 1, 48–49 (1976) (per curiam)).

Here, by contrast, the Act is not grounded in any congressional aim to correct a perceived viewpoint imbalance on the TikTok platform by achieving a different ideological mix. Congress, as discussed, did not seek to prevent covert content manipulation by the PRC in furtherance of any overarching objective of suppressing (or elevating) certain viewpoints, messages, or content. *Supra* pp. 14–16. Instead, Congress’s objective was to protect our national security from the clandestine influence operations of a designated foreign adversary, regardless of the possible implications for the mix of views that may appear on the platform.

While that alone sets this case apart from *NetChoice*, *see* 144 S. Ct. at 2408 n.10, it also bears emphasis that the laws at issue in *NetChoice* did not serve a distinct interest entirely unrelated to the suppression of free expression. Here, on the other hand, the Act rests in significant measure on Congress’s data-protection interest, an interest indisputably having no relation to the suppression of speech. For that reason as well, *NetChoice* poses no obstacle to concluding that the Act serves important governmental interests for purposes of intermediate scrutiny.

2.

The Act’s divestment mandate is narrowly tailored to achieve Congress’s important national-security interests in preventing the PRC from accessing U.S. TikTok users’ data

and covertly manipulating content on the platform. The Act will bring about the severing of PRC control of the TikTok platform in the United States, either through a divestment of that control, or, if no qualifying divestment takes place, through a prohibition on hosting or distributing a still-PRC-controlled TikTok in the United States until a qualifying divestment occurs. The divestment mandate is “not substantially broader than necessary to achieve” Congress’s national-security objectives. *Ward*, 491 U.S. at 800.

Congress confined the Act to applications subject to the control of just four designated foreign adversary countries, including China. § 2(g)(4); *see* 10 U.S.C. § 4872(d)(2). As applied here, the divestment mandate is fashioned to permit the TikTok platform—including its recommendation engine—to continue operating in the United States. *Supra* p. 10. Insofar as the PRC’s (or ByteDance’s) own decisions may prevent that from happening, the independent decisions of those foreign actors cannot render Congress’s chosen means substantially overbroad.

TikTok submits that various alternate means—including its proposed National Security Agreement (NSA), *see Op., ante*, at pp. 13–15—would equally fulfill Congress’s aims without giving rise to the prospect of the platform’s suspended operations in the United States. But even if we thought that were true, it would not help TikTok under intermediate scrutiny: under that standard, “[s]o long as the means chosen are not substantially broader than necessary,” a law “will not be invalid simply because a court concludes that the government’s interest could be adequately served by some less-speech-restrictive alternative.” *Ward*, 491 U.S. at 800; *see Turner II*, 520 U.S. at 217–18. A court instead must “defer to [Congress’s] reasonable determination” of how “its interest[s] . . . would be best served.” *Ward*, 491 U.S. at 800.

Here, Congress reasonably determined that attaining the requisite degree of protection required mandating a divestment of PRC control. A “disagreement over the level of protection . . . to be afforded and how protection is to be attained” does not constitute a basis for “displac[ing] Congress’ judgment” when applying intermediate scrutiny. *Turner II*, 520 U.S. at 224. And Congress’s resolution here is in line with other situations in which national-security concerns can call for divestment of a foreign country’s control over a U.S. company. *See* 50 U.S.C. § 4565(d)(1); H.R. Rep. No. 118-417, at 5–6 & n.26.

Nor could TikTok succeed under intermediate scrutiny by pointing to evidence that, in its view, contradicts Congress’s determination that nothing shy of divestment would be sufficient. TikTok argues, for instance, that in concluding the NSA was an inadequate alternative, the government misunderstood certain aspects of its design and operation—e.g., how difficult it would be to review TikTok’s source code. “[R]egardless of whether the evidence is in conflict” on such matters, a court can still sustain a challenged law when applying intermediate scrutiny. *Turner II*, 520 U.S. at 211. That is because “the relevant inquiry” under that standard is “not whether Congress, as an objective matter, was correct to determine [its chosen means are] necessary” to meet its objectives. *Id.*; *see id.* at 196. “Rather, the question is whether the legislative conclusion was reasonable and *supported by substantial evidence in the record before Congress.*” *Id.* at 211 (emphasis added). It was here.

The Executive Branch believed, and specifically advised Congress, that measures short of divestment would not adequately protect against the risks to national security posed by the PRC’s potential control of the TikTok platform. *See* Newman Decl. ¶ 7 (Gov’t App. 47); Redacted Hearing Tr. 11–

14. With specific regard to the provisions contained in the proposed NSA, “senior Executive Branch officials concluded that the terms of ByteDance’s final proposal would not sufficiently ameliorate those risks.” Newman Decl. ¶ 6 (Gov’t App. 46). The provisions, in the Executive Branch’s view, “still permitted certain data of U.S. users to flow to China, still permitted ByteDance executives to exert leadership control and direction over TikTok’s US operations, and still contemplated extensive contacts between the executives responsible for the TikTok U.S. platform and ByteDance leadership overseas.” *Id.* ¶ 75 (Gov’t App. 62). And, the Executive Branch assessed, the NSA “would have ultimately relied on . . . trusting ByteDance” to comply, but “the requisite trust did not exist.” *Id.* ¶¶ 75, 86 (Gov’t App. 62, 68).

Those concerns about the kinds of provisions in the NSA and the overarching lack of trust were discussed with Congress. *See* Redacted Hearing Tr. 10–12, 40–42, 49–50. Congress’s reliance on those Executive Branch conclusions, even if they are now disputed by TikTok, means its “legislative conclusion was . . . supported by substantial evidence in the record before [it].” *Turner II*, 520 U.S. at 211; *see id.* at 198–99 (relying on conflicted testimony before Congress).

\* \* \* \* \*

While the court today decides that the Act’s divestment mandate survives a First Amendment challenge, that is not without regard for the significant interests at stake on all sides. Some 170 million Americans use TikTok to create and view all sorts of free expression and engage with one another and the world. And yet, in part precisely because of the platform’s expansive reach, Congress and multiple Presidents determined that divesting it from the PRC’s control is essential to protect our national security.



To give effect to those competing interests, Congress chose divestment as a means of paring away the PRC's control—and thus containing the security threat—while maintaining the app and its algorithm for American users. But if no qualifying divestment occurs—including because of the PRC's or ByteDance's unwillingness—many Americans may lose access to an outlet for expression, a source of community, and even a means of income.

Congress judged it necessary to assume that risk given the grave national-security threats it perceived. And because the record reflects that Congress's decision was considered, consistent with longstanding regulatory practice, and devoid of an institutional aim to suppress particular messages or ideas, we are not in a position to set it aside.

**United States Court of Appeals**  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

**No. 24-1113****September Term, 2024**

FILED ON: DECEMBER 6, 2024

TIKTOK INC. AND BYTEDANCE LTD.,

PETITIONERS

v.

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

RESPONDENT

---

Consolidated with 24-1130, 24-1183

---

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

---

Before: SRINIVASAN, *Chief Judge*, RAO, *Circuit Judge*, and GINSBURG, *Senior Circuit Judge*

**J U D G M E N T**

These causes came to be heard on the petitions for review of constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act and were argued by counsel. On consideration thereof, it is

**ORDERED** and **ADJUDGED** that the petitions for review be denied, in accordance with the opinion of the court filed herein this date.

**Per Curiam**

**FOR THE COURT:**  
Mark J. Langer, Clerk

BY: /s/

Daniel J. Reidy  
Deputy Clerk

Date: December 6, 2024

Opinion for the court filed by Senior Circuit Judge Ginsburg.  
Opinion concurring in part and concurring in the judgment filed by Chief Judge Srinivasan.

**JA 93**

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/>		)	

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**

---

BRIAN FIREBAUGH, CHLOE JOY  
SEXTON, TALIA CADET, TIMOTHY  
MARTIN, KIERA SPANN, PAUL  
TRAN, CHRISTOPHER TOWNSEND,  
and STEVEN KING,

Case No. 24-1130

*Petitioners,*

v.

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

*Respondent.*

---

**PETITION FOR REVIEW AND COMPLAINT  
FOR DECLARATORY AND INJUNCTIVE RELIEF**

## NATURE OF THE ACTION

1. Petitioners are among the 170 million Americans who create, publish, view, interact with, and share videos on TikTok. They rely on TikTok to express themselves, learn, advocate for causes, share opinions, create communities, and even make a living. Although they come from different places, professions, walks of life, and political persuasions, they are united in their view that TikTok provides them a unique and irreplaceable means to express themselves and form community. They bring this lawsuit to preserve their First Amendment rights and the rights of countless others, which are threatened by the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50 (Apr. 24, 2024).

2. The Act bans TikTok unless its owners divest the platform in a manner that is infeasible, as the company has stated and as the publicly available record confirms. The Act thus promises to shutter a discrete medium of communication that has become part of American life,<sup>1</sup> prohibiting Petitioners from creating and disseminating expressive material with their chosen editor and publisher—and from receiving such material from others.

3. This extraordinary restraint on speech violates the First Amendment. In supporting the Act, lawmakers claimed that TikTok “manipulate[s]” American

---

<sup>1</sup> Sapna Maheshwari, *TikTok Has Changed America*, N.Y. Times (Apr. 19, 2024), <https://tinyurl.com/3emzadbb>.

minds<sup>2</sup> and disseminates “propaganda” that would “use our country’s free marketplace to undermine our love for liberty.”<sup>3</sup> But it is the Act that undermines the nation’s founding principles and free marketplace of ideas. The First Amendment to our Constitution precludes Congress from censoring speech because of its content, viewpoints, editorial practices, or identity of speakers or publishers.

4. To the extent the government may claim the Act’s ban is necessary to protect Americans’ data, it has tried that strategy before and lost. Two federal district courts have found that such concerns do not justify a ban. And rightly so. The concerns are speculative, and even if they were not, they could be addressed with legislation much more narrowly tailored to any purported concern.

5. In sum, TikTok has a profound effect on American life. “Even if you’ve never opened the app, you’ve lived in a culture that exists downstream of what happens there.”<sup>4</sup> Petitioners are part of this. They have found their voices, amassed significant audiences, made new friends, and encountered new and different ways of thinking—all because of TikTok’s novel way of hosting, curating, and disseminating

---

<sup>2</sup> 170 Cong. Rec. H1163-71, H1169 (daily ed. Mar. 13, 2024) (statement of Rep. Dan Crenshaw), <https://tinyurl.com/2aac7du4>.

<sup>3</sup> Press Release, Rep. Mike Flood (NE), Congressman Flood Votes to Stop TikTok Propaganda (Mar. 13, 2024), <https://tinyurl.com/tw8zdns5>.

<sup>4</sup> Maheshwari, *supra* note 1; see also AJ Willingham et al., *The biggest ways TikTok has changed American culture*, CNN (Apr. 2, 2023), <https://tinyurl.com/mrjxnu8d>; Katerina Eva Matsa, *More Americans are getting news on TikTok, bucking the trend seen on most other social media sites*, Pew Rsch. Ctr. (Nov. 15, 2023), <https://tinyurl.com/yc3eyfc4>.



speech. The Act's ban of TikTok threatens to deprive them, and the rest of the country, of this distinctive means of expression and communication. Petitioners accordingly bring this action for declaratory and injunctive relief.

### **PARTIES**

6. Petitioner Brian Firebaugh is a first-generation rancher in Hubbard, Texas. After serving in the U.S. Marine Corps, Firebaugh experienced homelessness and addiction but eventually obtained treatment and got a job working in a hospital. Over time, Firebaugh was able to save up enough to buy a small ranch. He uses TikTok to educate the public and his 430,000 TikTok followers about agricultural issues, feature his ranch products, and help the ranching community through charitable endeavors. Firebaugh earns income from the TikTok Creator Fund<sup>5</sup> and selling ranch products promoted on the app, which has allowed him to become a full-time rancher. His TikTok success also opened the door to his participation in a recent Netflix game show where his winnings enabled him and his wife to afford the adoption process for their son.

7. Without access to TikTok, Firebaugh would need to get a different job and pay for daycare instead of raising his son at home. In his words, "if you ban TikTok, you ban my way of life." Without TikTok, Firebaugh will also lose an

---

<sup>5</sup> In 2020, TikTok launched a Creator Fund, which allows creators with a large following who consistently post content to receive awards from the TikTok Creator Fund. The Creator Fund has since evolved into the Creator Rewards Program.

important tool for helping his community and learning from and mentoring other ranchers. He has already started to see the effects of the Act, including a steep decline in new TikTok followers.

8. Petitioner Chloe Joy Sexton lives in Memphis, Tennessee. After losing her job in 2020, Sexton started creating videos on TikTok while raising a newborn baby and caring for her mother who was battling brain cancer. When her mother passed, Sexton adopted her seven-year-old sister and continued to create videos about parenting, mental health, and her true love: baking. Eventually, Sexton's success on TikTok allowed her to fulfill her lifelong dream of opening a cookie company—which has thrived, largely due to the loyalty of Sexton's 2.2 million TikTok followers, who have witnessed her journey. Sexton now ships thousands of cookies every week all over the world and has published her own cookbook.

9. Due to the Act, Sexton faces losing her vibrant community of TikTok followers who have consistently supported her throughout grief and the early days of parenthood, as well as celebrated her successes. Sexton would have to find another source of income and a different way of communicating to the public about her cookie company. TikTok's organic reach has allowed Sexton to connect with over two million people (who know and care about her content) for free—a powerful tool that traditional marketing cannot replicate.

10. Petitioner Talia Cadet lives in Capitol Heights, Maryland. She uses

TikTok to share her book reviews and promote Black authors, as well as Black-owned businesses throughout the country, with her more than 126,000 followers. Through TikTok, Cadet has connected with book lovers all over the country and been invited to host in-person author events. She cherishes building community on the app by amplifying minority voices and helping others discover her favorite local, independent businesses. Cadet also uses the app to express her creativity and share entertaining content about her daily life. The Act threatens to deprive Cadet of access to this powerful community that has come to mean so much to her and would prevent her from using her voice to most effectively promote the people and businesses that she cares about.

11. Petitioner Timothy Martin coaches college football in Mayville, North Dakota. He creates content on TikTok to share his love and knowledge of sports with his approximately one million followers. Martin started posting videos on TikTok in 2020 while working as a student athlete. He uses it to stay connected with others in the sports community and maintain a strong sense of identity and positive mental health. He enjoys expressing himself creatively on the app, in particular by making his signature sports-commentary videos using the green-screen feature in CapCut—a ByteDance product for video editing. Martin generates revenue from his TikTok videos and promotes recognition for the small-town university where he coaches football. Martin fears the ban will deprive him, as well as other former athletes who

use TikTok, of a valuable interactive community. It also threatens his supplemental income.

12. Petitioner Kiera Spann is a recent college graduate living in Charlotte, North Carolina. She started using TikTok in 2020 as a student to share information and ideas from her classes with the public. Today, Spann uses the app to advocate for the rights of sexual-assault survivors. She also educates her more than 760,000 TikTok followers about news, politics, and books. Spann partners with a variety of non-profits to spread awareness on TikTok about issues such as criminal justice reform and access to healthcare.

13. Because of the Act, Spann will lose her ability to share information and perspectives with hundreds of thousands of people around the country and the world. Indeed, Spann chooses TikTok in part because she finds it to be the best platform for connecting with other sexual-assault survivors and promoting awareness of victims' rights. Spann is concerned that the Act will deprive her of access to a critical forum for connecting with the communities that she has carefully cultivated over the past few years.

14. Petitioner Paul Tran lives in Atlanta, Georgia, where he and his wife founded a skincare line. After struggling to market their products through traditional advertising and other apps, the Trans found great success on TikTok, amassing 138,000 followers. The pair sell their line through TikTok Shop (TikTok's integrated

e-commerce solution that allows sellers to sell products directly on the platform). The couple's fame on TikTok has also led to life-changing opportunities, including appearances on television shows such as "Shark Tank" and "The Today Show." Without TikTok, such opportunities will disappear. Paul also uses TikTok to document memories with his young daughter, connect with other dads, follow martial arts, and research travel and restaurants.

15. Petitioner Christopher Townsend lives with his family in Philadelphia, Mississippi. He served in the U.S. Air Force for six years as a cryptologic language analyst. Townsend is now a well-known hip hop artist and founded an organization dedicated to promoting biblical literacy by quizzing individuals on their knowledge of stories from the Bible. Townsend shares videos of these light-hearted and informative biblical quizzes with his 2.5 million TikTok followers. He also uses the app to share his music, which addresses topics such as his religion, patriotism, and political views. Because of the Act, Townsend faces losing the platform on which he is able to express his beliefs and share his spirituality and music with the world.

16. Petitioner Steven King lives in Buckeye, Arizona. King has used TikTok since 2019 to create humorous content about his daily life and spread awareness about LGBTQ pride, self-confidence, and sober living. King also derives immense satisfaction and enjoyment from using his ingenuity to create content on the app for his 6.8 million followers—and seeing this content reach the kind of

audience that finds it most compelling. His content has deeply resonated with the public, some of whom ask King questions on TikTok about his experience coming out as gay in Arizona and his 28-year loving relationship with his husband. This community—which King has been unable to find on other social media and entertainment platforms—means the world to him.

17. King’s success on TikTok has opened up many opportunities for him, such as becoming a published author and being honored at the Cheer Choice Awards, which recognizes creators on social media who are making an impact using their platforms. Because of the Act, King is suddenly and unexpectedly facing the loss of his career and the irreplaceable community that he has worked hard to foster.

18. Respondent Merrick B. Garland is the Attorney General of the United States of America. The Act directs the Attorney General to bring actions enforcing its prohibitions.

## **JURISDICTION**

19. This Court has original jurisdiction over this matter under section 3(a)-(b) of the Act.

20. This Court also has authority under the Declaratory Judgment Act, 28 U.S.C. § 2201(a), to decide this action and award relief because the action presents an actual case or controversy within the Court’s original jurisdiction.

## BACKGROUND

### A. TikTok Provides a Distinct Medium for Expression.

21. TikTok is a popular online platform that allows users to create, watch, share, and interact with short-form videos. TikTok’s stated mission is to inspire creativity and bring joy.<sup>6</sup> More than one billion people around the world use TikTok each month, including approximately 170 million Americans.<sup>7</sup>

22. TikTok enables users to create, edit, and upload videos ranging from 15 seconds to 10 minutes in length. Users who create videos are called “creators,” while the term “users” refers to both content creators and consumers. TikTok provides creators a palette of tools to amplify their expression, such as sounds, filters, and special effects.<sup>8</sup> Creators have control and creative license over their videos. TikTok users can like, comment on, and share creators’ videos. The comment feature allows users to leave their impressions of or reactions to a TikTok video and facilitates conversation and community among users.

---

<sup>6</sup> TikTok, *Our Mission*, <https://tinyurl.com/6neyxe2e>.

<sup>7</sup> TikTok, *Thanks a billion!* (Sept. 27, 2021), <https://tinyurl.com/mr2e2rmv>; (@TikTokPolicy), X (Apr. 17, 2024, 6:56 PM), <https://tinyurl.com/4v293w4k>.

<sup>8</sup> Researchers have found that TikTok is “far more successful in converting content consumers into creators, in part because its creator tools are superior and more fun.” Arvind Narayanan, *TikTok’s Secret Sauce*, Knight First Amend. Inst. at Colum. Univ. (Dec. 15, 2022), <https://tinyurl.com/44d4ejse>; see also Werner Geyser, *What Is TikTok?—Everything You Need to Know in 2024*, Influencer Mktg. Hub (Jan. 30, 2024), <https://tinyurl.com/5798vp2x> (describing how TikTok’s tools support “creative freedom”); Mia Sato, *TikTok’s latest feature lets users make AR filters*, The Verge (Nov. 16, 2023), <https://tinyurl.com/vkvdw3mc> (describing TikTok’s “filter templates” that allow users to “experiment with more than 2,000 assets to use in their effects”).

23. Although TikTok is sometimes compared to other social media platforms, it is different in important ways. TikTok does not require users to create personal profiles with information about their backgrounds, likes, interests, education, employment, and relationship status, or to “follow” or “friend” other users. Instead, TikTok’s “For You” page provides curated videos for each user, without appending related user profile information or dates, making everything feel new and interesting. Unlike other platforms, TikTok allows users to explore new content and creators without personalizing their feeds themselves. “After years of irrelevant, disconnected news feeds, TikTok has revamped the scrolling experience, enabling discovery and curating interest-based entertainment.”<sup>9</sup>

24. These features are powered by the platform’s distinct content recommendation system, which curates a unique and personalized compilation of videos for individual users based on judgments from how they interact with videos about what types of content are likely to be most interesting to them. The recommendation system amplifies creators’ voices in different and distinct ways, providing them with an organic reach not just to more viewers but to specific viewers. This encourages creators to produce authentic expression and enables

---

<sup>9</sup> AJ Kumar, *How TikTok Changed the Social Media Game With Its Unique Algorithm*, Entrepreneur (Aug. 16, 2022), <https://tinyurl.com/2mks2euy>; see also James Broughel, *TikTok Is A Beacon Of Democracy In The Social Media Landscape*, Forbes (Apr. 19, 2024), <https://tinyurl.com/4ksur28w> (describing how TikTok’s algorithm “surface[s] content based on engagement with internet trends rather than metrics indirectly tied to follower count”).



viewers to receive more engaging content.<sup>10</sup> By “learning users’ interests and preferences in real time as they interact with content, it’s not unusual for videos created by everyday people to suddenly get millions of views[.]”<sup>11</sup> In effect, TikTok creates a universe where everyday Americans from all walks of life can connect, communicate, and find their communities just by being themselves. Visibility on TikTok is not driven by someone’s fame or fortune but by connections inspired by individual authentic expression.

25. For example, in 2020, Firebaugh had only 5,000 followers and was struggling to maintain his ranch. One day, after being inspired by another TikTok creator to share his ranching experience, he created a video to dispel the myth that all Longhorn cattle are “vicious and dangerous,” by showing him petting one of his friendly cattle. The video went viral and was viewed over 72,000 times, driving curious users to ask Firebaugh questions about agriculture and livestock and fueling interest in his way of life. This moment contributed to Firebaugh’s rise as a content creator on TikTok, magnifying his ability to connect with others and receive life-

---

<sup>10</sup> See Narayanan, *supra* note 8 (“TikTok’s algorithm treats each video more or less independently to assess its viral potential, caring relatively little about how many followers the creator has.”).

<sup>11</sup> Willingham et al., *supra* note 4; see also Caroline Petrow-Cohen, *L.A. influencers, businesses live or die on TikTok’s algorithm. Now they fear for the future*, L.A. Times (May 6, 2024), <https://tinyurl.com/yv98bzxv> (describing how TikTok supports creators and businesses without “a big production budget” and “bring[s] the viewers to them”); James Broughel, *TikTok Ban Lands a Blow to Intellectual Discourse Online*, Forbes (Apr. 30, 2024), <https://tinyurl.com/3c5stmbt> (TikTok’s “algorithm has demonstrated a remarkable ability to elevate content from a wide range of users, regardless of their prior popularity or follower count.”).

changing opportunities.

26. Likewise, a few years ago, Spann posted a TikTok video of a protest regarding a domestic violence assault, which went viral and was viewed approximately nine million times. This video and the resulting media coverage—as well as Spann’s continued advocacy—resulted in the perpetrator being held accountable and meaningful reforms in Spann’s community.

27. TikTok’s content recommendation system also fosters communities and opens doors for connection. Creators post videos on myriad topics, including art, science, comedy, pets, cooking, music, travel and tourism, psychology, politics, and current events. Users can discover new interests. And users with niche interests can find other enthusiasts. Indeed, on TikTok, “[n]o interest is too small or obscure to coalesce into a community.”<sup>12</sup> “Groups that specialize in, for instance, little-known cultural art forms or environmental conservation can reach new audiences, creating a mutually beneficial exchange” resulting in more awareness and more engaging content.<sup>13</sup>

28. Spann and Cadet, for example, participate in BookTok, a large, well-known community of readers who share and engage with TikTok videos reviewing,

---

<sup>12</sup> Willingham et al., *supra* note 4.

<sup>13</sup> *Id.*

recommending, and joking about the books they read.<sup>14</sup> Firebaugh has connected with other agricultural educators and cattle ranchers—a group that he described as insular. Firebaugh has called upon this community to help others in need. For example, he relied on TikTok to raise donations of badly needed cattle feed to send to the Texas panhandle after a recent series of devastating fires, and to alert the public about where to access his beef donations in cities around the state. Likewise, King has connected with other LGBTQ creators and audiences, as well as individuals living in or working through sobriety.

29. TikTok has also emerged as a forum for political advocacy. Politicians from across the spectrum use the platform, especially to reach young people, activate new supporters, and break out as candidates. Even after passage of the Act, United States Senators continue to use TikTok to express their views and reach their constituents.<sup>15</sup> The campaign for President Biden also uses TikTok, a practice that Rob Flaherty, the campaign’s deputy manager, defended when he stated on April 24, 2024, that it “would be silly to write off any place where people are getting information about the president.”<sup>16</sup>

---

<sup>14</sup> Ryan Hudgins, *21 popular BookTok books and why they went viral*, Today (Mar. 15, 2023), <https://tinyurl.com/kkvj3xur>.

<sup>15</sup> See, e.g., Sen. Ed Markey (@senmarkey), TikTok, <https://tinyurl.com/msxmmv5c>; Team Rosen (@rosenhq), TikTok, <https://tinyurl.com/3kxcrtf8>.

<sup>16</sup> Will Weissert, *Biden just signed a bill that could ban TikTok. His campaign plans to stay on the app anyway*, AP (Apr. 24, 2024), <https://tinyurl.com/4n5y3546>.

30. Petitioners also use TikTok to engage in political speech. For example, Townsend has participated in TikTok’s “Conservative Hype House,” a collective of creators who discuss and debate views on current events from a conservative perspective and take turns posting videos to the collective’s followers. Spann also uses TikTok to encourage Americans to engage in political and social advocacy.

31. Additionally, Petitioners use TikTok for information about news and current events. For example, King views news from national and international journalists on TikTok. He finds TikTok to be one of the most unbiased and unfiltered news sources. Likewise, in Spann’s experience, TikTok has a unique ability to spread time-sensitive and important news faster than any other platform—and she relies on it for such updates.

32. TikTok also provides distinctive tools, such as sounds, filters, and special effects, to allow creators to post content that is not entirely replicable on other platforms. Content created on TikTok and CapCut may look and sound different than content created elsewhere. For example, TikTok allows users to quickly react to other videos through “duets,” which allows creators to post their own videos alongside other TikTok videos; “stitches,” which allows them to clip and integrate scenes from other TikTok videos into their own; and “remixes,” which allow creators to “remix” different videos on TikTok. Many also use the app’s “green screen” feature, in which their heads float over an image or a video in the

style of a news presenter, to offer criticism or commentary. Unlike other services where professional creators upload high-cost productions, TikTok creators can—and often do—become viral sensations with simple and spontaneous videos.<sup>17</sup>

33. Firebaugh creates all his videos using TikTok because he finds the experience of creating videos through TikTok much easier than on other social media apps. Spann edits all her videos in TikTok or CapCut, finding other platforms inefficient. Likewise, Martin creates most of his videos using CapCut and relies heavily on the green-screen feature for his sports commentary videos. Without access to TikTok or CapCut, Martin would no longer be able to create his signature videos.

34. These characteristics—intrinsic to the medium and derived from the system TikTok uses to curate content for each user—give TikTok a distinct culture and identity. Creating videos on TikTok (“TikToks”) is thus its own form of expression, and content expressed through TikTok may convey a different meaning than content expressed elsewhere.

35. Not only is TikTok a *medium* for expression, it is also a *forum* shaped by its editorial values. The platform compiles expression from millions around the

---

<sup>17</sup> See, e.g., Frances Gurney, *This man has gone viral on TikTok for dancing to Nelly Furtado in front of his bathroom sink*, The Tab (Feb. 25, 2022), <https://tinyurl.com/yc45ttt5>; Jillian Giandurco, *Alex Consani Is TikTok's 2024 It Girl*, Bustle (Jan. 9, 2024), <https://tinyurl.com/22j6bxyt>.

world and curates the content through its recommendation system to create personalized compilations for each user. These compilations set TikTok apart from other platforms, which produce different compilations based on their own distinct editorial rules. Indeed, other social media platforms have attempted to recreate TikTok's "secret sauce" without the same success.<sup>18</sup>

36. In fact, all of the Petitioners have tried using other social media apps, with far less success. For example, King has 6.8 million followers on TikTok, but only about 137,000 on Facebook. Sexton has 2.2 million followers on TikTok, but only about 44,000 on Instagram. Townsend has 2.5 million followers on TikTok, but only about 298,000 on Instagram. Firebaugh has more than 430,000 followers on TikTok, but only about 22,000 on Instagram. Martin has one million followers on TikTok, but only about 10,000 on Instagram. Spann has over 760,000 followers on TikTok, but less than 10,000 on Instagram. Tran's company has 138,000 followers on TikTok, but less than 2,000 followers on Facebook. And Cadet has 126,000 followers on TikTok, but less than 7,000 on Instagram.

37. Sexton has compared TikTok with other social media apps by posting the same videos on multiple platforms. Her videos performed vastly better on

---

<sup>18</sup> Mia Sato, *YouTube is adding a slew of new TikTok-like features to Shorts*, The Verge (Aug. 1, 2023), <https://tinyurl.com/y9ssbvz5>; Conor Murray, *TikTok Clones: How Spotify, Instagram, Twitter And More Are Copying Features Like The 'For You' Page*, Forbes (Mar. 13, 2023), <https://tinyurl.com/5yp2s4ej>; Chris Stokel-Walker, *How TikTok beat Instagram*, Bus. Insider (Feb. 2, 2023), <https://tinyurl.com/25eh5zpb>.

TikTok. Sexton attributes these differences to the fact that TikTok’s algorithm, in her experience, gets her videos in front of the exact communities who find it most compelling—in her case, mostly mothers and fellow baking aficionados. Martin has experienced the same results—unlike other social media apps, TikTok conveys his content directly to sports lovers who are most likely to enjoy it.

38. TikTok’s defining traits stem from the editorial decisions it makes using its proprietary content recommendation technology. “TikTok would no longer be TikTok” without that technology.<sup>19</sup> Petitioners have personally experienced ownership and editorial changes that alter expression on other social media platforms, while also affecting the types of expression those platforms published and promoted.<sup>20</sup> For example, King and Spann no longer regularly post content on X after Elon Musk’s acquisition of Twitter. Spann worries that, if forced to divest, TikTok’s new owner may follow other social media companies and, for example, allow paid political advertising on the app, which fundamentally changes the user experience.

---

<sup>19</sup> Daniel E. Sanger, *TikTok Has Changed America*, N.Y. Times (Apr. 19, 2024), <https://tinyurl.com/3emzadbb>.

<sup>20</sup> Steven Lee Myers, et al., *The Consequences of Elon Musk’s Ownership of X*, N.Y. Times (Oct. 28, 2023), <https://tinyurl.com/3bstx77m> (“the site has experienced a surge in racist, antisemitic and other hateful speech”); Bobby Allyn, *Why can’t Twitter and TikTok be easily replaced? Something called ‘network effects’*, NPR (Apr. 12, 2023), <https://tinyurl.com/ymeummzy> (“Since Elon Musk acquired the platform in October, [one user] has noticed his Twitter feed devolve into an engine of self-promotion for the billionaire’s constantly shifting whims.”).

39. Petitioners thus have an interest not only in creating and accessing expression through TikTok, but an interest in creating and accessing expression as curated using TikTok's current editorial practices.

#### **B. Courts Block Attempts to Ban TikTok.**

40. TikTok has for years drawn regulatory scrutiny.<sup>21</sup> This scrutiny has focused on unproven data security claims stemming from the allegation that TikTok is a company whose ultimate parent is allegedly headquartered in China, as well as concerns about TikTok's resulting editorial choices, content, and viewpoints.<sup>22</sup> Federal courts have blocked every attempt to ban TikTok, including on the basis of unproven data security concerns.

41. In *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73 (D.D.C. 2020), the U.S. District Court for the District of Columbia held that the President lacked authority to issue an executive order intended to stop U.S. users from communicating on TikTok, even where the order's purported ultimate purpose was to protect national security by preventing China from accessing data. *Id.* at 83. While the court found ample evidence that China *generally* poses a credible national security threat, it found no "specific evidence" of a threat stemming from TikTok, much less that a

---

<sup>21</sup> See, e.g., John D. McKinnon, *U.S. Threatens Ban if TikTok's Chinese Owners Don't Sell Stakes*, WSJ (Mar. 15, 2023), <https://tinyurl.com/yxuus85z>.

<sup>22</sup> *Id.*



ban was the “only effective way to address that threat.” *Id.* at 85. The court later affirmed that conclusion as applied to additional Commerce Department regulations, enjoining the Secretary’s action and again finding a lack of evidence that TikTok posed a national security threat. *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 114–15 (D.D.C. 2020)

42. Similarly, in *Marland v. Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020), the U.S. District Court for the Eastern District of Pennsylvania enjoined the same executive order and related agency action. Rejecting the government’s national security concerns as “hypothetical,” the court concluded the public interest in an injunction outweighed the speculative risk the Government presented. *Id.* at 642–43.

43. Most recently, in *Alario v. Knudsen*, -- F. Supp. 3d --, 2023 WL 8270811, at \*8 (D. Mont. Nov. 30, 2023), the U.S. District Court for the District of Montana enjoined a law banning TikTok in Montana, holding the ban likely violated the company’s and users’ First Amendment rights and finding the state’s claim that Chinese officials could “gain access to Montanans’ data without their consent” unsupported by evidence. *Id.* at \*13.

44. In response to concerns raised by the government, TikTok has announced numerous measures to safeguard U.S. user data and protect the U.S. TikTok platform against foreign government influence. TikTok reports that it has voluntarily invested more than \$2 billion to build a system of technological and

governance protections, sometimes referred to as “Project Texas.” TikTok has also reported making additional commitments in a proposed 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 authority to suspend TikTok in the United States if the company were found to violate certain agreed-upon obligations.

**C. Congress Bans TikTok Unless the Company Finds, and the President Approves, a New Publisher.**

45. Undeterred, Congress has now banned TikTok in the United States, effective January 19, 2025. President Biden signed the Act on April 24, 2024.

46. The content-based, viewpoint-based, and speaker-based aims of the Act are no secret. In supporting the Act, Representative Crenshaw (TX) claimed TikTok “manipulate[s] the minds of Americans.”<sup>23</sup> Representative Smith (N.J.) described the Act as “countering [Chinese] efforts to sway [American] public opinion in its favor[.]”<sup>24</sup> Representative Flood (NE) claimed TikTok disseminates “propaganda” that would “use our country’s free marketplace to undermine our love for liberty.”<sup>25</sup> Representative Fulcher (ID) claimed TikTok gives China “the ability to engage in

---

<sup>23</sup> 170 Cong. Rec. at H1169.

<sup>24</sup> *Id.*

<sup>25</sup> Flood, *supra* note 3.

psychological warfare against the American people.”<sup>26</sup> Representative Strong (AL) asserted that TikTok “set[s] an anti-American narrative in the United States,” pushes “propaganda videos from Osama bin Laden,” and promotes “an anti-Israel message[.]”<sup>27</sup> One of the bill’s co-sponsors, Representative Krishnamoorthi (IL), claimed that “the CCP has ultimate control of the algorithm which feeds the content of the platform.”<sup>28</sup> And in an interview with Secretary of State Antony Blinken, Senator Mitt Romney (UT) explained that the Act enjoyed “overwhelming support” in Congress precisely because of members’ perceptions about the subject matter and viewpoints discussed on the platform, such as “the number of mentions of Palestinians relative to other social media” on “TikTok broadcasts.”<sup>29</sup>

47. These arguments focus on censoring TikTok’s content recommendation system. Without any evidence, certain Congressmembers created a fiction that TikTok curates content to push propaganda<sup>30</sup> and “drive certain

---

<sup>26</sup> Press Release, Rep. Russ Fulcher (ID), Congressman Russ Fulcher’s Statement on the Passage of H.R. 7521 (Mar. 14, 2024), <https://tinyurl.com/mwaunwda>.

<sup>27</sup> Press Release, Rep. Dale Strong (AL), Strong Statement on Curtailing CCP Surveillance on American Citizens (Mar. 13, 2024), <https://tinyurl.com/bddv4s89>.

<sup>28</sup> Rep. Raja Krishnamoorthi (IL), (@congressmanraja), Instagram (Apr. 25, 2024), <https://tinyurl.com/ycxw6xpf>.

<sup>29</sup> Press Release, Sec’y of State, Antony J. Blinken, Secretary Antony J. Blinken At McCain Institute’s 2024 Sedona Forum Keynote Conversation with Senator Mitt Romney (May 3, 2024), <https://tinyurl.com/57zafh8j>.

<sup>30</sup> Press Release, Rep. Jack Bergman (MI), Bergman Supports Bipartisan Legislation to Stop Foreign Adversaries from Owning Social Medial Companies (Mar. 13, 2024), <https://tinyurl.com/23j8st77>.

messages to divide Americans, to destabilize our politics, to influence policymakers to denigrate policymakers, [and] to tear our country apart.”<sup>31</sup> Representative Gallagher (WI)—who co-authored an earlier version of the Act—urged colleagues to support the Act precisely because TikTok had become a “dominant news platform” to which young Americans increasingly turn for news and information.<sup>32</sup> Because the same could be said of other social media, Congress’s decision to focus on TikTok demonstrates animus toward the speech TikTok publishes and the speakers who publish it.

48. Congressmembers’ concerns with content on TikTok extend beyond alleged foreign propaganda. Senator Warner (VA) lauded the bill for arresting what he called TikTok’s “enormous power to influence and divide Americans.”<sup>33</sup> Representative Clarke (NY) claimed the Act is necessary to force TikTok “to become an American company guided by American principles and Western democratic values,”<sup>34</sup> and Representative Huffman (CA) expressed concern about

---

<sup>31</sup> Scott Wong et al., *It could be months before the Senate takes up a TikTok bill, despite warnings about China*, NBC News (Mar. 20, 2024), <https://tinyurl.com/njsz2zar>.

<sup>32</sup> 170 Cong. Rec. at H1165.

<sup>33</sup> Press Release, Sen. Mark R. Warner (VA), Warner, Rubio Applaud House Passage of Bill to Protect Americans from Foreign Adversary Controlled Applications Including TikTok (Mar. 13, 2024), <https://tinyurl.com/3v9p7zxn>.

<sup>34</sup> Press Release, Rep. Yvette D. Clarke (NY), Rep. Clarke Releases Statement on H.R. 7521, The Protecting Americans from Foreign Adversary Controlled Applications Act (Mar. 7, 2024), <https://tinyurl.com/393xz8zb>.

the use of TikTok to wield “significant influence over tens of millions of Americans,” through “malign disinformation campaigns.”<sup>35</sup> Senator Cantwell (WA), who chairs the Senate subcommittee for technology, was even more explicit, suggesting the Act will allow the federal government to “stop bad actors from broadcasting ... into the United States with nefarious messages[.]”<sup>36</sup>

49. The Act bans a “foreign adversary controlled application” from operating (i.e., publishing) within the territorial borders of the United States. *See* Act § 2(a)(1)(A)-(B). The statute then makes clear (if it was not already clear) that it targets one particular company: TikTok. It expressly defines “foreign adversary controlled application” to include any application operated by TikTok or its ultimate parent, ByteDance Ltd. *Id.* § 2(g)(3)(A)(i)-(iii).

50. The Act also makes clear its focus is the speech TikTok publishes. While the Act singles out TikTok, it establishes a more general category of “covered compan[ies]” to which it can theoretically apply. *Id.* § 2(g)(2)(A). Even for such companies, the Act applies only to entities that operate an application with more than one million monthly active users during a specified time period that enables those

---

<sup>35</sup> Press Release, Rep. Jared Huffman (CA), Huffman Statement On Vote For The Protecting Americans From Foreign Adversary Controlled Applications Act (Mar. 12, 2024), <https://tinyurl.com/mtrbmmze>.

<sup>36</sup> Natalie Andrews, *Powerful Senator Crafts TikTok Crackdown*, WSJ (Apr. 14, 2024), <https://tinyurl.com/kpdsyatm>.

users to “generate, share, and view text, images, videos, real-time communications, or similar content.” *Id.* And the Act expressly excludes from that catchall definition of “covered company” any companies that offer any service “whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.” *Id.* § 2(g)(2)(B).

51. The Act contains a so-called “qualified divestiture” regime that underscores its purpose and effect is to ban TikTok. *Id.* § 2(g)(6). The Act provides that TikTok may theoretically continue publishing in the United States if sold within 270 days to another approved entity. *Id.* § 2(a)(1)(A), § 2(a)(2)(A), § 2(g)(6). The President possesses discretion to withhold pre-approval, as the Act ultimately leaves it to his judgment—following an unspecified “interagency process”—whether to approve the divestiture. *Id.* § 2(g)(6)(B). But to the extent the Act includes standards to guide the President’s discretion, they make clear the Act effectuates a ban. Specifically, the Act requires the President to ensure that any divested successor is not permitted to maintain “any operational relationship” between its 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.” *Id.* TikTok states this is not a viable option. *See* Pet. for Review ¶¶ 25-29, *TikTok Inc. v. Garland*, No. 24-1113 (D.C. Cir. May 7, 2024).

Publicly available information reinforces that conclusion.<sup>37</sup>

52. The Act subjects any entity that provides access to TikTok in violation of this ban to a penalty of \$5,000 for each user who access the platform “multipl[ie]d ... by the number of users within the land or maritime borders of the United States” who access, maintain, or update the app as a result of the violation. *Id.* § 2(d)(1)(A). Because TikTok currently has approximately 170 million users in the United States, the fine for continuing to enable access to TikTok would be roughly \$850 billion.

### LEGAL PRINCIPLES

53. Only certain strictly limited categories of speech fall outside the First Amendment’s protection—defamation, fraud, incitement, true threats, obscenity, and speech integral to criminal conduct—and the Supreme Court has repeatedly rejected attempts to expand these categories. *United States v. Stevens*, 559 U.S. 460, 468-69 (2010). The First Amendment protects Americans’ rights to distribute and receive all other information, including from overseas. *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965).

54. Prior restraints—that is, restraints on speech before it is published—are the most serious and the least tolerable infringement on First Amendment rights. *Neb. Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976). Any law that imposes a prior

---

<sup>37</sup> Laura He, *Banning TikTok would hit China’s tech ambitions and deepen the global digital divide*, CNN (Apr. 24, 2024), <https://tinyurl.com/bdp8mk74>.

restraint on expression thus carries “a heavy presumption against its constitutional validity,” *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963), even where the restraint is allegedly necessary for national security, *N.Y. Times Co. v. United States*, 403 U.S. 713, 714 (1971).

55. Content-based, viewpoint-based, and speaker-based laws that restrict or burden speech are also presumptively unconstitutional. The “government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.” *Brown v. Ent. Merchs. Ass’n*, 564 U.S. 786, 790–91 (2011) (citation omitted). Nor may the government discriminate among speakers, particularly where such restrictions “reflect the Government’s preference for the substance of what the favored speakers have to say (or aversion to what the disfavored speakers have to say).” *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 658 (1994). Finally, the Government may not require speakers to use editors or publishers different from those with whom the speakers wish to associate and work. *See Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos.*, 515 U.S. 557, 569–70 (1995).

56. Any law that restricts speech along any of these lines is subject to strict or an even higher form of scrutiny, requiring, at a minimum, that the government establish that its regulation furthers a compelling interest and uses the least restrictive means to achieve it. *United States v. Playboy Ent. Grp.*, 529 U.S. 803, 813 (2000).



57. Even intermediate scrutiny—which applies where laws restrict merely the time, place, or manner of speech—requires the government to prove its restriction (1) will serve a substantial government interest “unrelated to the suppression of free expression” by alleviating in a direct and material way harms that are “not merely conjectural,” and (2) is narrowly tailored to suppress no more speech “than is essential to the furtherance of that interest.” *Turner*, 512 U.S. at 662, 664 (citations omitted).

58. The Constitution also “gives significant protection from overbroad laws that chill speech within the First Amendment’s vast and privileged sphere.” *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 244 (2002). Even if a law has some legitimate applications, it still is unconstitutional if “a substantial number of its applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Stevens*, 559 U.S. at 473 (citation omitted). Laws categorically banning protected speech are thus virtually always invalid because they are overbroad. *See Bd. of Airport Commr’s of City of L.A. v. Jews for Jesus*, 482 U.S. 569, 574–75 (1987).

### **CLAIM ONE**

#### **VIOLATION OF THE FIRST AMENDMENT TO THE U.S. CONSTITUTION**

59. Petitioners incorporate all prior allegations above as if fully set forth herein.

60. The Act regulates “speech” under the First Amendment by singling out and effectively banning a medium of communication—TikTok—that Petitioners (and other Americans) use to engage in protected expression, prohibiting them from sending and receiving information they are entitled to communicate.

61. The Act erects an unconstitutional prior restraint by banning protected speech on TikTok and by empowering the President to pre-approve who may publish and edit TikTok’s service and, in turn, the speech Petitioners wish to disseminate on that platform.

62. The Act regulates on a content-, speaker-, and viewpoint-basis. The law is content- and speaker-based because it expressly bans TikTok but exempts other companies based on the type of content those companies’ apps publish. The law is also content-, speaker-, and viewpoint-based because it prohibits operation of TikTok’s current content recommendation system by its current editors, preventing Petitioners from using their chosen editor and publisher to engage in protected communication. From the standpoint of the First Amendment, this restriction is no different from prohibiting American freelance writers from submitting articles to *The Economist*, or American musicians from disseminating songs through Spotify. The Act further regulates speech based on its viewpoint because it is motivated by a disfavored view of the ideas that are, or could be, expressed or promoted on TikTok.

63. The Act for all these reasons bears a heavy presumption of

unconstitutionality—more stringent than even strict scrutiny—and fails even intermediate scrutiny. The government cannot ban a medium for communication because it believes that medium is used to transmit foreign “propaganda” or other protected content. Nor does the government have any actual, non-speculative evidence that banning TikTok in its current form enhances Americans’ data security, or that its ban is narrowly tailored to accomplish that objective. The fact that the Act is paired with other federal legislation restricting how data brokers may share and sell American user information to certain foreign entities underscores that the ban is not narrowly tailored.

64. The government has not identified any other basis to justify its ban, nor is there any conceivable legitimate interest that would warrant shuttering an entire media platform used by millions that could not be achieved through narrower regulation.

65. The Act is unconstitutionally overbroad because it bans an entire medium of communication and all the speech communicated through that medium, even though, at the very least, the vast majority of that speech is protected and not otherwise subject to suppression.

66. Unless declared invalid and enjoined, the Act will unlawfully deprive Petitioners of their rights under the First Amendment, inflicting immediate and irreparable harm.

**PRAYER FOR RELIEF**

WHEREFORE, Petitioners respectfully pray for judgment:

- a. Granting this Petition for Review;
- b. Declaring the Act invalid under the United States Constitution

because it violates Petitioners' First Amendment rights;

- c. Enjoining Respondent from taking any action to enforce the Act;
- d. Entering judgment in favor of Petitioners; and
- e. Awarding Petitioners all other such relief as the Court deems just

and proper.

Dated: May 14, 2024

DAVIS WRIGHT TREMAINE LLP

By: /s/ Ambika Kumar  
Ambika Kumar

Ambika Kumar  
Tim Cunningham  
DAVIS WRIGHT TREMAINE LLP  
920 Fifth Avenue, Suite 3300  
Seattle, Washington 98104  
(206) 757-8030  
ambikakumar@dwt.com  
timcunningham@dwt.com

Jeffrey L. Fisher  
O'MELVENY & MYERS LLP  
2765 Sand Hill Road  
Menlo Park, California 94025  
(650) 473-2633  
jlfisher@omm.com

Elizabeth A. McNamara  
Chelsea T. Kelly  
DAVIS WRIGHT TREMAINE LLP  
1251 Avenue of the Americas  
New York, New York 10020

(212) 489-8230  
lizmcnamara@dwt.com  
chelseakelly@dwt.com

James R. Sigel  
Adam S. Sieff  
DAVIS WRIGHT TREMAINE LLP  
50 California Street, Suite 2300  
San Francisco, California 94111  
(415) 276-6500  
jamessigel@dwt.com  
adamsieff@dwt.com

*Attorneys for Petitioners*

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

---

BASED POLITICS INC.,

Petitioner,

v.

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

Respondent.

---

No. 24-1183

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

## INTRODUCTION

1. TikTok is a social media platform on which millions of Americans publish and consume *speech*. Some of that speech might be considered frivolous—such cat videos, trendy dances, or people lip syncing to popular songs. But much of the speech on TikTok is serious, addressing important political and social issues. And all of it is protected by the First Amendment.

2. Petitioner BASED Politics Inc. is a nonprofit organization established in part to reach Gen Z with educational content and commentary from a perspective that favors free markets and individual liberty.

3. Its founders, Hannah Cox and Brad Polumbo, use TikTok to communicate with that audience, including thousands of young people who otherwise would never hear their message. Their videos on topics such as systemic racism, the gender pay gap, economics, and free speech typically receive thousands of views—some hundreds of thousands, and some more than a million.

4. Their use of TikTok also allows them to engage with their audience, receiving feedback and debating ideas raised in their videos.

5. Now, however, the federal government has enacted a law that will shut down TikTok—and, with it, the ability of BASED Politics to reach its audience with its message—unless this Court enjoins its enforcement.

6. This is a petition for review of that statute, the Protecting Americans from Foreign Adversary Controlled Applications Act (“the Act”), Pub. L. No. 118-50, Div. H (Apr. 24, 2024), attached to this Petition as Exhibit 1.

7. Petitioner asks this Court to declare the statute unconstitutional and enjoin the Respondent, Attorney General Merrick Garland, from enforcing it. An injunction against the Act is essential to prevent irreparable harm to the First Amendment rights of Petitioner and the millions of other Americans who use TikTok to publish and consume protected speech.

### **PARTIES**

8. Petitioner Based Politics Inc. is a Georgia 501(c)(3) nonprofit organization that publishes educational content on free markets and individual liberty, including, among other things, articles, podcasts,



social media posts, and TikTok videos by its founders, Hannah Cox and Brad Polumbo.

9. Respondent Merrick Garland is the United States Attorney General, charged by the Foreign Adversary Controlled Applications Act with the statute's enforcement.

### **JURISDICTION AND VENUE**

10. This Court has original jurisdiction over this matter under Section 3(a)-(b) of the Foreign Adversary Controlled Applications Act, which provides that all challenges to that Act must be brought in this Court.

11. This Court also has authority under the Declaratory Judgment Act, 28 U.S.C. § 2201(a), to decide this action and award relief because the action presents an actual case or controversy within the Court's original jurisdiction.

### **FACTUAL ALLEGATIONS**

#### **TikTok**

12. TikTok is an online video hosting platform on which users can publish and view videos that typically range in length from 15 seconds to three minutes.

13. More than 170 million Americans use TikTok to publish and consume speech, including political speech.

14. More Americans use TikTok than Pinterest, LinkedIn, Snapchat, X (formerly Twitter), Discord, Threads, Truth Social, or Mastodon. Brian Fung, *Biden Just Signed a Potential TikTok Ban Into Law. Here's What Happens Next*, CNN, April 24, 2024.<sup>1</sup>

15. TikTok's algorithm shows each user an ongoing selection of curated videos on their "For You" page feed.

16. This system gives each TikTok user his or her own unique feed of videos selected by TikTok's algorithm, based on the user's reactions to and engagement with other videos the user has seen on the platform.

17. In this way, TikTok's algorithm allows users to find content they might not actively search for, which can allow TikTok content creators to more easily reach an interested audience.

18. TikTok is owned by ByteDance Ltd., a company incorporated in the Cayman Islands and headquartered in Beijing, China.

---

<sup>1</sup> <https://www.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html>  
(last accessed May 27, 2024)

## **Petitioner's Use of TikTok for Speech**

19. Petitioner BASED Politics Inc. is a 501(c)(3) nonprofit organization established in part to reach Gen Z with social media content that promotes free markets and individual liberty. BASED Politics publishes its content on various internet platforms, including TikTok.

20. BASED Politics President and co-founder Hannah Cox relies on TikTok to bring the organization's message to viewers who are not otherwise accessible on other social media platforms. Her TikTok account has amassed some 43,000 followers, and her TikTok videos on topics including systemic racism and the gender pay gap have reached hundreds of thousands, and even as many as one million, people at a time.

21. BASED Politics co-founder Brad Polumbo, a journalist, uses TikTok on the organization's behalf to publish educational videos on topics ranging from higher education to economics to free speech. He has accumulated more than 15,000 followers, and his videos received more than 1.5 million views from April 4 to June 4, 2024 alone.

22. The TikTok algorithm has introduced BASED Politics content to thousands of unique individuals who likely never would have heard its

message anywhere else because many members of Gen Z get news exclusively from TikTok.

23. TikTok's unique content curation algorithm affords Petitioner an opportunity to reach an audience that it could not reach on other social media platforms—both because TikTok has users who do not use the other platforms, and because some TikTok audience members would not seek out or otherwise see **BASED** Politics content when using other platforms.

24. Petitioner's reach on TikTok is a direct result of TikTok's proprietary content curation algorithm.

25. Many TikTok users have used TikTok to send Cox and Polumbo messages or comments of support, or to engage in debate about their videos.

### **The Foreign Adversary Controlled Applications Act**

26. On April 24, 2024, President Biden signed into law The Foreign Adversary Controlled Applications Act, H.R. 815, 118th Cong. (2024) (the "Act")—a statute that effectively bans TikTok in the United States.

27. The Act makes it unlawful to “provid[e] services to distribute, maintain, or update” a “foreign adversary controlled application” “within the land or maritime borders of the United States,” by either of two ways. Act § 2(a)(1)(A).

28. First, the Act makes it illegal to distribute, maintain, or update a “foreign adversary controlled application” by “providing services to distribute, maintain, or update such” applications “by means of a market place (including an online mobile application store) through which users within the land or maritime borders of the U.S. may access, maintain, or update [it].” *Id.*

29. Thus, for example, the Act would make it unlawful for the Apple Store to allow users to download and update a foreign adversary controlled application.

30. Second, the Act makes it illegal for a website hosting service to host data for a “foreign adversary controlled application.” *Id.* at § 2(a)(1)(B).

31. The Act provides that TikTok may continue to operate if ByteDance makes a “qualified divestiture” of the platform within 270 days of the Act’s enactment—that is, by January 19, 2025. *Id.* § 2(c)(1).

32. The Act defines a “qualified divestiture” to include “a divestiture or similar transaction” that the President determines, through an interagency process, (A) “would result in [TikTok] no longer being controlled by a foreign adversary” and (B) “precludes the establishment or maintenance of any operational relationship between the United States operations of [the platform] and any formerly affiliated entities that are controlled by a foreign agency, including any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing.” *Id.* § 2(g)(6).

33. In other words, the Act provides that app stores may only continue to allow access to TikTok, and U.S. hosting services may only host TikTok, if its current owners sell it to an entity not controlled by a “foreign adversary” by January 19, 2025.

34. That deadline is subject to a single extension of 90 days if the President certifies to Congress that “(A) a path to executing a qualified divestiture has been identified with respect to [the] application”; “(B) evidence of significant progress” toward the divestiture “has been produced”; and (C) “there are in place binding legal agreements to enable

execution of such qualified divestiture during the period of such extension.” *Id.* § 2(a)(3).

35. The Act gives the President authority to determine whether TikTok’s buyer is a foreign adversary or controlled by a foreign adversary. *Id.* § 2(g)(6).

36. ByteDance has stated that it will not sell TikTok, notwithstanding the Act. Aimee Picchi, *After Biden Signs TikTok Ban into Law, ByteDance Says it Won’t Sell the Social Media Service*, CBS NEWS, April 26, 2024.<sup>2</sup>

37. If ByteDance does not sell TikTok, then the Act will effectively shut TikTok down within the United States on January 19, 2025.

### **Purported Justifications for the Act**

38. One justification federal legislators have advanced for the Act is that TikTok allegedly poses a threat to American national security.

39. For example, Senate Commerce Committee Chairwoman Maria Cantwell has said that the Act’s purpose is to “prevent foreign adversaries from conducting espionage, surveillance, maligned

---

<sup>2</sup> <https://www.cbsnews.com/news/tiktok-bytedance-says-it-wont-sell/> (last accessed May 24, 2024)

operations, harming vulnerable Americans, our servicemen and women, and our U.S. government personnel.” Haleluya Hadero, *Senate Passes Bill Forcing TikTok’s Parent Company to Sell or Face Ban, Sends to Biden for Signature*, ASSOCIATED PRESS, April 23, 2024.<sup>3</sup>

40. House Foreign Affairs Committee Chairman Michael McCaul has called TikTok “a spy balloon in Americans’ phones,” which can “surveil and exploit America’s personal information.” Cristiano Lima-Strong and Taylor Telford, *House Passes Potential TikTok Ban that Could Speed Through Senate*, THE WASHINGTON POST, April 20, 2024.<sup>4</sup>

41. Another ostensible justification for the Act is that TikTok pushes propaganda.

42. For example, Representative Mike Flood stated that TikTok “has been used as a tool of propaganda in our country.” *Press Release*, MIKE FLOOD, March 13, 2024.<sup>5</sup> And Senator Marco Rubio stated that “[t]he Marxist bias on TikTok reflects more than left-wing thought among

---

<sup>3</sup> <https://apnews.com/article/tiktok-ban-congress-bill-1c48466df82f3684bd6eb21e61ebcb8d> (last accessed May 27, 2024)

<sup>4</sup> <https://www.washingtonpost.com/technology/2024/04/20/tiktok-ban-vote-house-passes/> (last accessed May 27, 2024)

<sup>5</sup> <https://flood.house.gov/media/press-releases/congressman-flood-votes-stop-tiktok-propaganda> (last accessed May 27, 2024)



millennials and Generation Z. It reflects the app's subservience to the world's most powerful Marxist regime: the Chinese Communist Party.”

Marco Rubio, *Pro-Hamas TikTok Videos Hint at a Broader Chinese Influence Campaign*, WASHINGTON EXAMINER, Nov. 10, 2023.<sup>6</sup>

43. The Office of the Director of National Intelligence has further alleged that “TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties during the U.S. midterm election cycle in 2022.” Mallory Culhane, *The Chinese Government is Using TikTok to Meddle in Elections, ODNI Says*, POLITICO, March 11, 2024.<sup>7</sup>

44. In addition, some have alleged that TikTok censors content on issues on which the Chinese government is particularly sensitive, such as Tiananmen Square, Tibetan independence, and Falun Gong. Alex Hern, *Revealed: How TikTok Censors Videos that do not Please Beijing*, THE GUARDIAN, Sept. 25, 2019.<sup>8</sup>

---

<sup>6</sup> <https://www.washingtonexaminer.com/opinion/beltway-confidential/2779399/pro-hamas-tiktok-videos-hint-at-a-broader-chinese-influence-campaign/> (last accessed May 27, 2024).

<sup>7</sup> <https://www.politico.com/news/2024/03/11/china-is-using-tiktok-for-influence-campaigns-odni-says-00146336> (last accessed May 27, 2024)

<sup>8</sup> <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing> (last accessed May 27, 2024)

45. The purported justifications for the ban based on TikTok's alleged use for propaganda reveal that the Act exists to punish TikTok for its editorial decisions and thus imposes a content-based restriction on speech.

## **CLAIMS FOR RELIEF**

### **COUNT ONE**

#### **The Act violates the First Amendment of the United States Constitution.**

46. Petitioner incorporates the preceding paragraphs by reference.

47. The Act regulates speech by effectively banning a medium of communication—TikTok—that Petitioner uses to engage in protected political speech.

48. Petitioner's speech on TikTok is core speech protected by the First Amendment.

49. The Act constitutes a prior restraint on speech by prohibiting U.S. internet hosting services from hosting speech published on TikTok.

50. The Act constitutes a prior restraint on speech by prohibiting app stores and others from making TikTok available within the United States, thus preventing TikTok from publishing that speech to people within the United States.

51. The Act constitutes a prior restraint on speech by empowering the President to pre-approve TikTok's buyer—and therefore TikTok's next editor—and thus determine the type (content) of speech that will be published on TikTok.

52. As a prior restraint, the Act carries “a ‘heavy presumption’ against its constitutional validity.” *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971) (quoting *Carroll v. Princess Anne*, 393 U.S. 175, 181 (1968)).

53. By forcing ByteDance to either sell TikTok to an approved buyer or shut it down within the U.S., the Act burdens Petitioner's free-speech rights by prohibiting Petitioner from publishing its videos to its audience.

54. The Act also prohibits Petitioner from publishing on its chosen platform *through that platform's chosen editor*—and through the algorithm that currently delivers Petitioner's speech to its audience.

55. The Act violates the First Amendment because it is overbroad: it bans all speech communicated on TikTok, even though all, or almost all, of it is speech protected by the First Amendment that the government has no legitimate interest in censoring.

56. Purported concerns about national security and protecting Americans from propaganda cannot justify banning TikTok.

57. Although the government of the People's Republic of China might represent a threat to United States national security, there is no evidence to support allegations that TikTok threatens national security.

58. To the extent that TikTok could be shown to pose a threat to national security, the Act's ban on all speech on TikTok is not narrowly tailored to serve the government's interest in addressing that threat.

59. Thus, even if national security is a compelling government interest, the Act's ban on TikTok in its current form is not narrowly tailored to serve that interest, and national security therefore cannot justify the Act's infringement of First Amendment rights.

60. Further, the suppression of "propaganda"—that is, censorship of speech based on its political content—is not a legitimate government

interest, let alone a compelling one, and cannot justify the Act's infringement of First Amendment rights.

### **PRAYER FOR RELIEF**

WHEREFORE, Petitioner respectfully requests that this Court:

- A. Grant this Petition for Review;
- B. Declare the Act invalid because it violates Petitioner's First Amendment right to freedom of speech;
- C. Enjoin Respondent from enforcing the Act;
- D. Enter a judgment in favor of Petitioner; and
- E. Award Petitioner any and all other relief the Court deems just and proper.

Dated: June 6, 2024

Respectfully submitted,

**LIBERTY JUSTICE CENTER**

By: /s/ Jacob Huebert

Jacob Huebert  
Jeffrey Schwab  
James McQuaid  
LIBERTY JUSTICE CENTER  
13341 W. U.S. Highway 290  
Building 2  
Austin, Texas 78737  
(512) 481-4400  
jhuebert@ljc.org  
jschwab@ljc.org  
jmcquaid@ljc.org

Attorneys for Petitioner  
BASED Politics Inc.

118TH CONGRESS } 2d Session }	HOUSE OF REPRESENTATIVES	{ REPORT 118-417
----------------------------------	--------------------------	---------------------

---

PROTECTING AMERICANS FROM FOREIGN ADVERSARY  
CONTROLLED APPLICATIONS ACT

MARCH 11, 2024.—Committed to the Committee of the Whole House on the State  
of the Union and ordered to be printed

Mrs. RODGERS of Washington, from the Committee on Energy and  
Commerce, submitted the following

R E P O R T

[To accompany H.R. 7521]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 7521) to protect the national security of the United States from the threat posed by foreign adversary controlled applications, such as TikTok and any successor application or service and any other application or service developed or provided by ByteDance Ltd. or an entity under the control of ByteDance Ltd., having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

	Page
Purpose and Summary .....	2
Background and Need for Legislation .....	2
Committee Action .....	12
Committee Votes .....	12
Oversight Findings and Recommendations .....	14
New Budget Authority, Entitlement Authority, and Tax Expenditures .....	14
Congressional Budget Office Estimate .....	14
Federal Mandates Statement .....	14
Statement of General Performance Goals and Objectives .....	14
Duplication of Federal Programs .....	14
Related Committee and Subcommittee Hearings .....	14
Committee Cost Estimate .....	15
Earmark, Limited Tax Benefits, and Limited Tariff Benefits .....	15
Advisory Committee Statement .....	15
Applicability to Legislative Branch .....	15
Section-by-Section Analysis of the Legislation .....	15
Changes in Existing Law Made by the Bill, as Reported .....	18

## PURPOSE AND SUMMARY

Communications applications that are owned and operated by companies controlled by foreign adversary countries present a clear threat to the national security of the United States. This is because such applications can be used by those countries to collect vast amounts of data on Americans, conduct espionage campaigns, and push misinformation, disinformation, and propaganda on the American public.

The United States has, for more than 100 years, restricted foreign governments and persons from owning media outlets and holding broadcast licenses. However, current law does not address the situation where a foreign adversary country has significant control over a company that operates a technology application, even where such application poses a significant threat to national security.

H.R. 7521, the “Protecting Americans from Foreign Adversary Controlled Applications Act” protects Americans from national security risks posed certain by applications controlled by a foreign adversary of the United States. If an application is determined to be a foreign adversary controlled application, such as TikTok’s parent company ByteDance, the application must be divested so that it is no longer in the foreign adversary’s control. If the application is not divested within 180 days, entities in the United States would be prohibited from distributing the application through an application marketplace or store, and from providing web hosting services. The 180 days would begin upon enactment of the legislation for ByteDance, TikTok, and other subsidiaries; for other foreign adversary controlled applications, the 180 days begins after a Presidential determination that the application poses a significant threat to national security. The legislation includes a requirement that foreign adversary controlled applications provide users, upon request, information related to the user’s account, including photos, videos, and posts, in a machine-readable format. This Act addresses the immediate national security risks posed by TikTok and establishes a framework for the Executive Branch to protect Americans from future foreign adversary controlled applications.

## BACKGROUND AND NEED FOR LEGISLATION

Communications technologies and networks underpin the daily lives of the American public and economy. Foreign adversaries have used access to Americans’ data, communications networks, devices, and applications as entry points to disrupt Americans’ daily lives, conduct espionage activities, and push disinformation and propaganda campaigns in an attempt to undermine our democracy and gain worldwide influence and control. This is all a detriment to our national security interests.

One such adversary that has aggressively pursued this strategy is the People’s Republic of China (PRC). It has backed hackers to disrupt our communications networks<sup>1</sup> and used “deceptive and coercive methods” to shape global information. As described by the U.S. Department of State, its goals are to promote “digital authoritarianism.”<sup>2</sup> They have accomplished some of these goals

<sup>1</sup> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

<sup>2</sup> <https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/>.



through coercion of companies headquartered in the PRC. One way it does so is through its National Intelligence Law of 2017, which requires PRC individuals and entities to support PRC intelligence services, including by providing data without regard to where that data was collected and without any mechanism of due process.<sup>3</sup>

Beijing ByteDance Technology is a Chinese internet technology company headquartered in Beijing and operating in the United States through a holding company (“ByteDance Ltd.”) incorporated in the Cayman Islands.<sup>4</sup> ByteDance Ltd., founded and headquartered in Beijing, was formed in 2012 and launched a number of applications and products which became extremely popular, including TikTok.<sup>5</sup>

TikTok is now one of the most popular social media platforms in the world. It is available in over 150 countries and serves over 1 billion users.<sup>6</sup> In the United States, TikTok has over 170 million users and is especially popular among teenagers and young adults who represent 35 percent of its American user base.<sup>7</sup>

Foreign adversary controlled applications present a clear threat to the national security of the United States. This includes TikTok due to ByteDance, Ltd.’s ownership of the application.<sup>8</sup>

Outside reporting has indicated the breadth of TikTok’s reach, suggesting that its data collection practices extend to age, phone number, precise location, internet address, device used, phone contacts, social network connections, the content of private messages sent through the application, and videos watched.<sup>9</sup> The risk posed by TikTok though is exacerbated by the difficulty in assessing precisely which categories of data it collects. For example, outside researchers have found embedded vulnerabilities that allow the company to collect more data than the app’s privacy policy indicates.<sup>10</sup>

Additionally, public reporting has repeatedly confirmed statements made by the Executive Branch regarding the tight interlinkages between ByteDance Ltd., TikTok, and the Chinese Communist Party (CCP). For example, the Secretary of ByteDance Ltd.’s CCP committee, Zhang Fuping, also serves as ByteDance Ltd.’s Editor-in-Chief and Vice President and has vowed that the CCP committee would “take the lead” across “all product lines and business lines,” which includes TikTok.

<sup>3</sup> U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF STRATEGY, POLICY & PLANS, DATA SECURITY BUSINESS ADVISORY: RISKS AND CONSIDERATIONS FOR BUSINESSES USING DATA SERVICES AND EQUIPMENT FROM FIRMS LINKED TO THE PEOPLE’S REPUBLIC OF CHINA at 6 (December 22, 2020), [https://www.dhs.gov/sites/default/files/publications/20\\_1222\\_data-security-business-advisory.pdf](https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf).

<sup>4</sup> Beijing ByteDance Technology and its Cayman Island holding company, ByteDance Ltd., will interchangeably be referred to as “ByteDance.”

<sup>5</sup> Joe Tidy and Sophia Smith Galer, *TikTok: The story of a social media giant*, BBC News (5 August 2020), <https://www.bbc.com/news/technology-53640724>.

<sup>6</sup> *TikTok Statistics For 2024: Users, Demographics, Trend*, What’s The Big Data (Nov. 29, 2023), <https://whatsthebigdata.com/tiktok-statistics/>.

<sup>7</sup> Jamie Ding, *Why TikTok is dangerously good at making you spend money*, L.A. Times (Dec. 3, 2023), <https://www.latimes.com/business/story/2023-12-03/why-tiktok-is-dangerously-good-at-making-you-spend-money>.

<sup>8</sup> Judy Woodruff, *CIA Director Bill Burns on War in Ukraine, Intelligence Challenges Posed by China*, PBS (Dec. 16, 2022, 6:50 P.M.), <https://www.pbs.org/newshour/show/cia-director-bill-burns-on-war-in-ukraine-intelligence-challenges-posed-by-china>.

<sup>9</sup> Geoffrey A. Fowler, *Is it time to delete TikTok? A guide to the rumors and the real privacy risks*, WASH. POST (July 13, 2020), <https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/>. See also Office of the Director of National Intelligence, *National Counterintelligence and Security Center, “Operations Security (OPSEC) Advisory, TikTok Concerns and Vulnerabilities”* (Mar. 2023), [https://www.dni.gov/files/NCSC/documents/nittf/OPSEC\\_Advisory\\_TikTok\\_Concerns\\_and\\_Vulnerabilities.pdf](https://www.dni.gov/files/NCSC/documents/nittf/OPSEC_Advisory_TikTok_Concerns_and_Vulnerabilities.pdf).

<sup>10</sup> Fowler, *supra* note 2.

Moreover, pursuant to the PRC's laws, the PRC can require a company headquartered in the PRC to surrender all its data to the PRC, making companies headquartered there an espionage tool of the CCP:

- The National Intelligence Law, passed in China in 2017, requires that “any organization” must assist or cooperate with CCP intelligence work.<sup>11</sup> Such assistance or cooperation must also remain secret at the PRC's request.<sup>12</sup>
- The PRC's 2014 Counter-Espionage Law requires that “relevant organizations . . . may not refuse” to collect evidence for an investigation.<sup>13</sup>
- The PRC's Data Security Law of 2021 establishes that the PRC has the power to access and control private data.<sup>14</sup>
- The PRC's Counter-Espionage Law grants PRC security agencies nearly unfettered discretion, if acting under an unrestricted understanding of national security, to access data from companies.<sup>15</sup>

As a result, the Department of Homeland Security has warned that “[t]he PRC's data collection actions result in numerous risks to U.S. businesses and customers, including: the theft of trade secrets, of intellectual property, and of other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service; security and privacy risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses.”<sup>16</sup> These risks are imminent, but other, unforeseen risks may also exist.

Prior to 2022, several federal agencies, including the Departments of Defense, State, and Homeland Security, issued orders banning TikTok on devices for which those specific agencies are responsible.<sup>17</sup> A majority of states in the United States have banned TikTok on state government devices due to the national security threat posed by the application under its current ownership.<sup>18</sup>

As has been widely reported, TikTok has proposed an alternative to a ban, a proposal referred to as “Project Texas,” which is an initiative to try and satisfy concerns relating to TikTok's handling of U.S. user data. This proposal was rolled out in July 2022. Under the proposal, U.S. user data would be stored in the United States, using the infrastructure of a trusted third party.<sup>19</sup> How-

<sup>11</sup> Joe McDonald & Zen Soo, *Why Does US See Chinese-Owned TikTok as a Security Threat?*, AP NEWS (Mar. 24, 2023, 10:24 A.M.), <https://apnews.com/article/tiktok-bytedance-shou-zi-chew-8d8a6a9694357040d484670b7f4833be>.

<sup>12</sup> U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF STRATEGY, POLICY & PLANS, DATA SECURITY BUSINESS ADVISORY: RISKS AND CONSIDERATIONS FOR BUSINESSES USING DATA SERVICES AND EQUIPMENT FROM FIRMS LINKED TO THE PEOPLE'S REPUBLIC OF CHINA at 6 (December 22, 2020), [https://www.dhs.gov/sites/default/files/publications/20\\_1222\\_data-security-business-advisory.pdf](https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf).

<sup>13</sup> McDonald & Soo, *infra* note 5.

<sup>14</sup> Code Civil, Data Security Law of the People's Republic of China, 2021, art (China).

<sup>15</sup> Library of Congress, China: Counterespionage Law Revised, <https://www.loc.gov/item/global-legal-monitor/2023-09-21/china-counterespionage-law-revised/>.

<sup>16</sup> DATA SECURITY BUSINESS ADVISORY, *supra* note 6.

<sup>17</sup> See, e.g., Neil Vigdor, “U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning,” N.Y. TIMES (Jan. 4, 2020), <https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html>.

<sup>18</sup> Sawdah Bhainmiya, *Here's a full list of the US states that have introduced full or partial TikTok bans on government devices over mounting security concerns*, Business Insider (Jan. 15, 2023, 5:00 AM), <https://www.businessinsider.com/tiktok-banned-us-government-state-devices-2023-1>.

<sup>19</sup> TikTok Response to Sen Blackburn, June 30, 2022, <https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1>, p.2.

ever, under the initiative, the application algorithm, source code, and development activities would remain in China under ByteDance Ltd.'s control and subject to PRC laws, subject to proposed safeguards relating to cloud infrastructure and other data security concerns. Project Texas would also allow ByteDance Ltd. to continue to have a role in certain aspects of TikTok's U.S. operations.<sup>20</sup>

Additionally, Project Texas would allow TikTok to continue to rely on the engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application in the U.S.<sup>21</sup> But allowing code development in and access to U.S. user data from China potentially exposes U.S. users to malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development. Furthermore, allowing back-end support, code development, and operational activities to remain in China would also require TikTok to continue to send U.S. user data to China to update the machine learning algorithms and source code for the application, and to conduct related back-end services, like managing users' accounts.<sup>22</sup>

As of March 2024, Project Texas has not been completed. Until Project Texas is complete, Beijing-based employees of TikTok can access U.S. user data.<sup>23</sup>

Finally, as TikTok's popularity continues to grow in the United States, so does the risk it poses. Attempted action by the Executive Branch to mitigate these risks has proven unsuccessful, and therefore Congress must act to provide congressional authority to protect U.S. national security.

Congress has previously taken such action with respect to media companies in passing the Communications Act of 1934, which limits foreign investment in television and radio broadcast licenses.<sup>24</sup> These foreign ownership restrictions were originally adopted to protect national security interests during wartime by preventing the airing of foreign propaganda on broadcast stations.<sup>25</sup> Today, applications like TikTok operate in similar manner as other media companies in the United States, and therefore they should be subject to foreign ownership scrutiny too.

Below is a list of public statements that have been made regarding the national security risks posed by ByteDance Ltd., TikTok, and the CCP as well as past and ongoing actions being taken to mitigate the national security risks associated with these entities and similarly situated companies:

- In May 2019, in connection with a review by the Committee on Foreign Investment in the United States (CFIUS), a company based in the PRC agreed to divest its interest in a popular software application reportedly due to concerns relat-

<sup>20</sup> See, e.g., *TikTok v. Trump*, 490 F.Supp.3d 73 (D.D.C. Sept. 27, 2020); *Marland v. Trump*, 20-cv-04597 (E.D. Pa. Sept. 18, 2020).

<sup>21</sup> *Id.*, p.3-5.

<sup>22</sup> See, e.g., Emily Baker White, EXCLUSIVE: TikTok Spied On Forbes Journalists, *Forbes* (December 22, 2022), <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=68c05b5d7da5>.

<sup>23</sup> Christianna Silva, What is Project Texas, TikTok's Best Chance to Avoid a Deal, *Mashable* (March 28, 2023), <https://mashable.com/article/project-texas-tiktok>.

<sup>24</sup> 47 U.S.C. 310(b).

<sup>25</sup> *In re Commission Policies and Procedures Under Section 310(b)(4) of the Communications Act, Foreign Investment in Broadcast Licenses*, 28 FCC Rcd 16244 (2013), <https://www.fcc.gov/document/fcc-clarifies-policy-foreign-investment-broadcast-licensees-0>.

ing to potential access by the PRC to American user data from the application.<sup>26</sup>

- On May 15, 2019, the President of the United States (President) issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which stated that “unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries . . . constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”<sup>27</sup>

- On August 2, 2020, then-Secretary of State Mike Pompeo stated that PRC-based companies “are feeding data directly to the Chinese Communist Party, their national security apparatus.”<sup>28</sup>

- On August 6, 2020, the President concluded that TikTok “automatically captures vast swaths of information from its users” and that TikTok’s ownership by ByteDance Ltd. enables the PRC and CCP to gain access to “Americans’ personal and proprietary information,” potentially allowing the CCP “to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.”<sup>29</sup>

- On August 6, 2020, the President issued an Executive Order (E.O. 13942) that directed the Secretary of Commerce to take actions that would have prohibited certain transactions related to TikTok in 45 days if ByteDance failed to divest its ownership of TikTok.<sup>30</sup> The companies and content creators using the TikTok mobile application filed lawsuits challenging those prohibitions, as a result of which two district courts issued preliminary injunctions enjoining the prohibitions.<sup>31</sup>

- On August 14, 2020, the President found “there is credible evidence . . . that ByteDance Ltd. . . . might take action that threatens to impair the national security of the United States.”<sup>32</sup>

- On August 14, 2020, the President issued an Executive Order directing ByteDance Ltd. to divest any assets or property used to enable or support ByteDance Ltd.’s operation of the TikTok application in the United States and any data ob-

<sup>26</sup>Zack Whittaker, *Grindr sold by Chinese owner after US raised national security concerns*, *Tech Crunch*. (March 6, 2020, 1:06 PM), <https://techcrunch.com/2020/03/06/grindr-sold-china-national-security/>.

<sup>27</sup>Exec. Order No. 13,873, 84 FR 22689 (May 15, 2019), <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>.

<sup>28</sup>Ronn Blitzer, *Pompeo Warns TikTok Users’ Personal Info Could Be Going Directly to the Chinese Communist Party*, *FOX NEWS* (Aug. 2, 2020, 12:39 P.M.), <https://www.foxnews.com/politics/pompeo-warns-tiktok-users-data-including-facial-pattern-residence-phone-number-could-be-going-directly-to-the-chinese-communist-party>.

<sup>29</sup>Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020), <https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency> (revoked by Exec. Order No. 14,034 (June 9, 2021), <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>).

<sup>30</sup>Exec. Order No. 13942, 85 Fed. Reg. 51297 (Aug. 6, 2020).

<sup>31</sup>*See, e.g., TikTok v. Trump*, 490 F.Supp.3d 73 (D.D.C. Sept. 27, 2020); *Marland v. Trump*, 20-cv-04597 (E.D. Pa. Sept. 18, 2020).

<sup>32</sup>Order of August 14, 2020, 85 Fed. Reg. 51,297 (Aug. 19, 2020), <https://www.govinfo.gov/content/pkg/FR-2020-08-19/pdf/2020-18360.pdf>.

tained or derived from TikTok application or musical.ly application users in the United States.<sup>33</sup> The Order, however, remains the subject of litigation.

- On September 17, 2020, the Department of Commerce concluded that the PRC, to advance “its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment,” is constructing “massive databases of Americans’ personal information” and that ByteDance Ltd. has close ties to the CCP, including a cooperation agreement with a security agency and over 130 CCP members in management positions.<sup>34</sup>

- Following the multiple judicial rulings that enjoined the Executive Branch from enforcing the regulations contemplated in E.O. 13942, on June 9, 2021, the President issued a new Executive Order that rescinded E.O. 13942 and directed the Secretary of Commerce to assess and take action, where possible, against connected software applications that pose a threat to national security more broadly.<sup>35</sup>

- On June 9, 2021, the President issued an Executive Order on Protecting Americans’ Sensitive Data from Foreign Adversaries, which stated that “[f]oreign adversary access to large repositories of United States persons’ data also presents a significant risk.”<sup>36</sup> The EO stated that “the United States must act to protect against the risks associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.”<sup>37</sup>

- On October 26, 2021, lawmakers expressed concerns that TikTok’s audio and user location data could be used by the CCP during the testimony of Michael Beckerman, TikTok head of public policy for the Americas and registered lobbyist for ByteDance Ltd., before a Senate Commerce Subcommittee on Consumer Protection hearing.<sup>38</sup>

- On June 17, 2022, public reporting revealed that leaked audio from more than 80 internal TikTok meetings, China-based employees of ByteDance Ltd. repeatedly accessed non-public data about U.S. TikTok users, including the physical locations of specific U.S. citizens.<sup>39</sup>

- On September 14, 2022, lawmakers expressed concerns over TikTok’s algorithm and content recommendations posing a national security threat during a hearing before the Senate

<sup>33</sup> Order of Aug. 14, 2020, “Regarding the Acquisition of Musical.ly By Bytedance Ltd.” 85 Fed. Reg. 51297 (Aug. 19, 2020).

<sup>34</sup> *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 78 (D.D.C. 2020) (mem.). [BETTER CITATION: U.S. Dep’t of Commerce, Mem. for the Sec’y, *Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942* (Sept. 17, 2020), ECF No. 22–1]

<sup>35</sup> Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 9, 2021).

<sup>36</sup> Exec. Order No. 14,034, 86 FR 31423 (Jun 9, 2021), <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>.

<sup>37</sup> *Id.*

<sup>38</sup> Diane Bartz & Sheila Dang, *TikTok Tells U.S. Lawmakers It Does Not Give Information to China’s Government*, REUTERS (Oct. 26, 2021, 4:53 P.M.), <https://www.reuters.com/technology/tiktok-tells-us-lawmakers-it-does-not-give-information-chinas-government-2021-10-26/>.

<sup>39</sup> Emily Baket-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEED. (June, 17, 2022), [HTTPS://WWW.BUZZFEEDNEWS.COM/ARTICLE/EMILYBAKERWHITE/TIKTOK-TAPES-US-USER-DATA-CHINA-BYTEDANCE-ACCESS](https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access).

Committee on Homeland Security and Governmental Affairs with Vanessa Pappas, Chief Operating Officer of TikTok.<sup>40</sup>

- On November 15, 2022, Federal Bureau of Investigation (FBI) Director Christopher Wray testified before the House Committee on Homeland Security that TikTok's national security concerns "include the possibility that the [CCP] could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so choose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices."<sup>41</sup>

- On December 2, 2022, FBI Director Wray stated that TikTok's data repositories on Americans "are in the hands of a government that doesn't share our values and that has a mission that's very much at odds with what's in the best interests of the United States. . . . The [CCP] has shown a willingness to steal Americans data on a scale that dwarfs any other."<sup>42</sup>

- On December 5, 2022, Director of National Intelligence Avril Haines stated, when asked about TikTok and PRC ownership, "It is extraordinary the degree to which [the PRC] . . . [is] developing [] frameworks for collecting foreign data and pulling it in, and their capacity to then turn that around and use it to target audiences for information campaigns and other things, but also to have it for the future so that they can use it for a variety of means."<sup>43</sup>

- On December 16, 2022, Central Intelligence Agency Director William Burns explained that "because the parent company of TikTok is a [PRC] company, the [CCP] is able to insist upon extracting the private data of a lot of TikTok users in this country, and also to shape the content of what goes on to TikTok as well to suit the interests of the Chinese leadership."<sup>44</sup>

- On December 22, 2022, public reporting revealed that ByteDance Ltd. employees accessed TikTok user data and IP addresses to monitor the physical locations of specific U.S. citizens.<sup>45</sup>

- On December 29, 2022, following its adoption by Congress, the President signed into law a bill banning the use of TikTok

<sup>40</sup> Vanessa Pappas, Testimony Before the U.S. Senate Committee on Homeland Security and Governmental Affairs, <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Pappas-2022-09-14-REVISED.pdf>.

<sup>41</sup> Ariana Figueroa, *Members of Congress Sign Up for TikTok, Despite Security Concerns*, IDAHO CAP. SUN (Jan. 19, 2023, 12:26 P.M.), <https://idahocapitalsun.com/2023/01/19/members-of-congress-sign-up-for-tiktok-despite-security-concerns/>.

<sup>42</sup> Anisha Kohli, *Why the FBI Is Concerned About TikTok*, TIME MAG. (Dec. 3, 2022, 3:42 P.M.), <https://time.com/6238540/tiktok-fbi-security-concerns/>.

<sup>43</sup> Transcript, Avril Haines, Dir. of Nat'l Intel., Fireside Chat with DNI Haines at the Reagan National Defense Forum (Dec. 3, 2022), <https://www.dni.gov/index.php/newsroom/news-articles/news-articles-2022/3660-fireside-chat-with-dni-haines-at-the-reagan-national-defense-forum>.

<sup>44</sup> Judy Woodruff, *CIA Director Bill Burns on War in Ukraine, Intelligence Challenges Posed by China*, PBS (Dec. 16, 2022, 6:50 P.M.), <https://www.pbs.org/newshour/show/cia-director-bill-burns-on-war-in-ukraine-intelligence-challenges-posed-by-china>.

<sup>45</sup> Emily Baker White, *EXCLUSIVE: TikTok Spied On Forbes Journalists*, *Forbes* (December 22, 2022), <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=68c05b5d7da5>.

on government devices due to the national security threat posed by the application under its current ownership.<sup>46</sup>

- On January 20, 2023, public reporting revealed that TikTok and ByteDance Ltd. employees regularly engage in practice called “heating,” which is a manual push to ensure specific videos “achieve a certain number of video views.”<sup>47</sup>

- In a court filing in June 2023, a former employee of ByteDance Ltd. alleged that the CCP spied on pro-democracy protestors in Hong Kong in 2018 by using backdoor access to TikTok to identify and monitor activists’ locations and communications.<sup>48</sup>

- On November 1, 2023, public reporting revealed that TikTok’s internal platform, which houses its most sensitive information, was inspected in person by CCP cybersecurity agents in the lead-up to the CCP’s 20th National Congress.<sup>49</sup>

- In February 2023, Deputy Attorney General Lisa Monaco stated, “Our intelligence community has been very clear about [the CCP’s] efforts and intention to mold the use of [TikTok] using data in a worldview that is completely inconsistent with our own.”<sup>50</sup> Deputy AG Monaco also stated, “I don’t use TikTok and I would not advise anybody to do so because of [national security] concerns.”<sup>51</sup>

- On February 28, 2023, former Deputy National Security Advisor Matthew Pottinger emphasized that it has already been confirmed that TikTok’s parent company ByteDance has used the app to surveil U.S. journalist as a means to identify and retaliate against potential sources. The PRC has also shown a willingness to harass individuals abroad who take stances that contradict the Communist Party lines.<sup>52</sup> The app can further be employed to help manipulate social discourse and amplify false information to tens of millions of Americans.<sup>53</sup>

<sup>46</sup> David Ingram, *Biden Signs TikTok Ban for Government Devices, Setting Up a Chaotic 2023 for the App*, NBC NEWS (Dec. 30, 2022, 4:24 P.M.), <https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724>.

<sup>47</sup> Emily Baker-White, *TikTok’s Secret ‘Heating’ Button Can Make Anyone Go Viral*, FORBES (Jan. 20, 2023), <https://www.forbes.com/sites/emilybaker-white/2023/01/20/tiktoks-secret-heating-button-can-make-anyone-go-viral/?sh=62d61d006bfd>.

<sup>48</sup> Brian Fung, *Analysis: There is now some public evidence that China viewed TikTok data*, CNN (June 8, 2023, 10:28 A.M.), <https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html>.

<sup>49</sup> Emily Baker-White, *A Platform Storing TikTok Corporate Secrets Was Inspected By The Chinese Government*, FORBES (Nov. 1, 2023, 6:30 A.M.), <https://www.forbes.com/sites/emilybaker-white/2023/11/01/a-platform-storing-tiktok-corporate-secrets-was-inspected-by-the-chinese-government/?sh=193ba64e23b2>.

<sup>50</sup> John D. McKinnon, *U.S. Threatens Ban if TikTok’s Chinese Owners Don’t Sell Stakes*, WALL ST. J. (Mar. 15, 2023, 6:45 P.M.), <https://www.wsj.com/articles/u-s-threatens-to-ban-tiktok-if-chinese-founder-doesnt-sell-ownership-stake-36d7295c>.

<sup>51</sup> Lauren Feiner, *High-Ranking DOJ Official Says She ‘Would Not Advise’ Consumers to Use TikTok, Citing Security Concerns*, CNBC (Feb. 16, 2023, 4:55 P.M.), <https://www.cnbc.com/2023/02/16/doj-lisa-monaco-warns-against-tiktok-use-citing-security-concerns.html>.

<sup>52</sup> On Hong Kong Authorities’ Transnational Repression, Press Statement, Anthony J. Blinken, Secretary of State (Dec. 15, 2023), <https://www.state.gov/on-hong-kong-authorities-transnational-repression/>; *Transnational Repression*, Freedom House, <https://freedomhouse.org/report/transnational-repression>; The PRC has also shown itself willing to harass Americans on U.S. soil. See, e.g., Josh Rogin, *Chinese police stations in NYC are part of a vast influence operation*, THE WASHINGTON POST (Apr. 19, 2023), <https://www.washingtonpost.com/opinions/2023/04/19/chinese-police-new-york-city-foreign-influence/>.

<sup>53</sup> Matthew Pottinger, Testimony Before the U.S. House Select Committee on the Chinese Communist Party, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2.28.2023-hearing-transcript.pdf>.

- On March 8, 2023, FBI Director Christopher Wray testified before the Senate Permanent Select Committee on Intelligence that the CCP, through its ownership of ByteDance, could use TikTok to collect and control users' data and drive divisive narratives internationally.<sup>54</sup>
- On March 22, 2023, elements of the intelligence community provided a classified briefing on the threat to members of the U.S. House of Representatives Permanent Select Committee on Intelligence and leadership of the Committee on Energy and Commerce.
- On March 23, 2023, Secretary of State Antony Blinken testified before the House Committee on Foreign Affairs that TikTok is a threat to national security that should be “ended one way or another.”<sup>55</sup>
- On March 23, 2023, during the testimony of TikTok CEO Shou Chew before the House Committee on Energy and Commerce, lawmakers expressed concerns about the safety and security of the app, including TikTok's relationship with the CCP.<sup>56</sup>
- On March 23, 2023, Nury Turkel, the Chair of the United States Commission on International Religious Freedom, raised the alarm that TikTok's parent company, ByteDance Ltd., has a strategic partnership with China's Ministry of Public Security, and China's domestic version of the app, Douyin, has been used to collect sensitive information from Uyghurs and other oppressed ethnic minority groups.<sup>57</sup>
- On April 26, 2023, the Executive Branch provided a classified briefing to members of the United States Senate Committee on Commerce, Science, and Transportation and the Senate Select Committee on Intelligence on the threat.
- On May 30, 2023, public reporting revealed that TikTok has stored sensitive financial information, including the Social Security numbers and tax identifications of TikTok influencers and United States small businesses, on servers in China accessible by ByteDance Ltd. employees.<sup>58</sup>
- On June 5, 2023, the Executive Branch provided a classified briefing to staff of the United States Senate Committee on Banking and the U.S. House of Representatives Committee on Energy and Commerce on the threat.
- In June 2023, at the request of the House Permanent Select Committee on Intelligence, the intelligence community provided a classified threat briefing open to all members in the U.S. House of Representatives.

<sup>54</sup> *FBI Chief Says TikTok 'Screams' of US National Security Concerns*, REUTERS (Mar. 9, 2023, 4:43 P.M.), <https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/>.

<sup>55</sup> Houston Keene, *Blinken Suggests TikTok 'Should Be Ended One Way or Another'*, FOX NEWS (Mar. 23, 2023, 6:11 P.M.), <https://www.foxnews.com/politics/blinken-tiktok-should-be-ended>.

<sup>56</sup> Dara Kerr, *Lawmakers Grilled TikTok CEO Chew for 5 Hours in a High-Stakes Hearing About the App*, NPR (Mar. 23, 2023, 5:34 P.M.), <https://www.npr.org/2023/03/23/1165579717/tiktok-congress-hearing-shou-zi-chew-project-texas>.

<sup>57</sup> Nury Turkel, *Testimony Before the U.S. House Select Committee on the Chinese Communist Party*, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/3.23.23-hearing-transcript.pdf>.

<sup>58</sup> Alexandra S. Levine, *TikTok Creators' Financial Info, Social Security Numbers Have Been Stored In China*, FORBES (May 30, 2023, 6:30 A.M.), <https://www.forbes.com/sites/alexandralevine/2023/05/30/tiktok-creators-data-security-china/?sh=1af8f2657048>.



- On July 26, 2023, William Evanina, the former director of the National Counterintelligence and Security Center, pointed to TikTok as just one of many areas of concern regarding the CCP's capabilities and intent as an adversarial, malign competitor.<sup>59</sup>
- On September 28, 2023, the U.S. Department of State's Global Engagement Center issued a report that found that "TikTok [c]reates [o]pportunities for PRC [g]lobal [c]ensorship. The report stated that U.S. Government information as of late 2020 showed that "ByteDance maintained a regularly updated internal list identifying people who were likely blocked or restricted from all ByteDance platforms, including TikTok, for reasons such as advocating for Uyghur independence."
- On November 15, 2023, elements of the intelligence community provided a classified briefing to the United States Senate Select Committee on Intelligence and the Committee on Commerce, Science, and Transportation on the PRC's conduct of global foreign malign influence operations, including through platforms such as TikTok.<sup>60</sup>
- On November 30, 2023, John Garnaut of the Australian Strategic Policy Institute remarked that TikTok has sophisticated capabilities that create the risk that TikTok can clandestinely shape narratives and elevate favorable opinions while suppressing statements and news that the PRC deems negative.<sup>61</sup>
- On January 18, 2024, the U.S. House of Representatives Select Committee on Strategic Competition between the United States and the Chinese Communist Party was briefed by a set of senior interagency officials to discuss these matters.
- On January 31, 2024, FBI Director Wray testified before the Select Committee on Strategic Competition between the United States and the Chinese Communist Party that TikTok gives the PRC "the ability to control data collection on millions of users, which can be used for all sorts of intelligence operations or influence operations," and "the ability, should they so choose, to control the software on millions of devices, which means the opportunity to technically compromise millions of devices."<sup>62</sup>
- On February 29, 2024, the U.S. House of Representatives Committee on Energy and Commerce was briefed by a set of senior interagency officials to discuss these matters.

<sup>59</sup>William Evanina, Testimony Before the U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/7.26.23-hearing-transcript.pdf>.

<sup>60</sup>Reuters, U.S. to Brief Senators on Foreign Online Influence Focused on Israel, Ukraine (November 15, 2023), <https://www.reuters.com/world/us/us-senators-get-classified-briefing-foreign-online-influence-2023-11-15/>.

<sup>61</sup>John Garnaut, Testimony Before the U.S. House Select Committee on the Chinese Communist Party, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/11.30.23-hearing-transcript.pdf>.

<sup>62</sup>The CCP Cyber Threat to the American Homeland and National Security, Hearing, The Select Committee on the CCP (March 1, 2024), <https://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american-homeland-and-national-security>.

## COMMITTEE ACTION

On March 23, 2023, the Committee on Energy and Commerce held a full committee hearing. The title of the hearing was “TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms.” The Committee received testimony from:

- Shou Chew, CEO, TikTok Inc.

On March 7, 2024, the Committee on Energy and Commerce held a full committee hearing to review H.R. 7521. The title of the hearing was “Legislation to Protect Americans from the National Security Threats Posed by Foreign Adversary Controlled Applications.” The Committee met in executive session pursuant to a motion by Chair Rodgers, which was adopted by a record vote of 43 yeas and 0 nays.

On March 7, 2024, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 7521 favorably reported, without amendment, to the House by a record vote of 50 yeas and 0 nays.

## COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The following reflects the record votes taken during the Committee consideration:

**COMMITTEE ON ENERGY AND COMMERCE  
118TH CONGRESS  
ROLL CALL VOTE # 1**

**BILL:** H.R. 7521, Prohibition of Foreign Adversary Controlled Applications Act

**AMENDMENT:** A motion by Chair Rodgers to order H.R. 7521, Prohibition of Foreign Adversary Controlled Applications Act favorably reported to the House, without amendment. (Final Passage)

**DISPOSITION:** AGREED TO, by a roll call vote of 50 yeas to 0 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Rep. Rodgers	X			Rep. Pallone	X		
Rep. Burgess	X			Rep. Eshoo	X		
Rep. Latta	X			Rep. DeGette	X		
Rep. Guthrie	X			Rep. Schakowsky	X		
Rep. Griffith	X			Rep. Matsui	X		
Rep. Bilirakis	X			Rep. Castor	X		
Rep. Bucshon	X			Rep. Sarbanes	X		
Rep. Hudson	X			Rep. Tonko	X		
Rep. Walberg	X			Rep. Clarke	X		
Rep. Carter	X			Rep. Cárdenas	X		
Rep. Duncan	X			Rep. Ruiz	X		
Rep. Palmer	X			Rep. Peters	X		
Rep. Dunn	X			Rep. Dingell	X		
Rep. Curtis	X			Rep. Veasey	X		
Rep. Lesko	X			Rep. Kuster	X		
Rep. Pence	X			Rep. Kelly	X		
Rep. Crenshaw	X			Rep. Barragán	X		
Rep. Joyce	X			Rep. Blunt Rochester			
Rep. Armstrong	X			Rep. Soto	X		
Rep. Weber	X			Rep. Craig	X		
Rep. Allen	X			Rep. Schrier	X		
Rep. Balderson	X			Rep. Trahan	X		
Rep. Fulcher	X			Rep. Fletcher	X		
Rep. Pfluger	X						
Rep. Harshbarger	X						
Rep. Miller-Meeks	X						
Rep. Cammack	X						
Rep. Obernolte	X						

03/07/2024

## OVERSIGHT FINDINGS AND RECOMMENDATIONS

Pursuant to clause 2(b)(1) of rule X and clause 3(c)(1) of rule XIII, the Committee held hearings and made findings that are reflected in this report.

## NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII, the Committee finds that H.R. 7521 would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

## CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII, at the time this report was filed, the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not available.

## FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

## STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to force a divestiture or prohibit the distribution, maintenance, or updating of foreign adversary controlled applications.

## DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 7521 is known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

## RELATED COMMITTEE AND SUBCOMMITTEE HEARINGS

Pursuant to clause 3(c)(6) of rule XIII, the following hearings were used to develop or consider H.R. 7521:

- On March 23, 2023, the Committee on Energy and Commerce held a full committee hearing. The title of the hearing was “TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms.” The Committee received testimony from:
  - Shou Chew, CEO, TikTok Inc.
- On March 7, 2024, the Committee on Energy and Commerce held a full committee hearing to review H.R. 7521. The title of the hearing was “Legislation to Protect Americans from the National Security Threats Posed by Foreign Adversary Controlled Applications.” The Committee met in executive session pursuant to a motion by Chair Rodgers, which was adopted by a record vote of 43 yeas and 0 nays.

## COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974. At the time this report was filed, the estimate was not available.

## EARMARK, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 7521 contains no earmarks, limited tax benefits, or limited tariff benefits.

## ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

## APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

## SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

*Section 1. Short title*

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

*Section 2. Prohibition of Foreign-Adversary Controlled Applications*

Subsection (a)(1) makes it unlawful for an entity to distribute, maintain, update, or enable the distribution, maintenance, or updating of a foreign adversary controlled application in the United States.

Subsection (a)(2) provides the applicable dates of prohibitions in subsection (a)(1), which is 180 days after enactment for the foreign adversary controlled applications in (g)(3)(A), and beginning 180 days after the relevant determination in (g)(3)(B) that such application poses an unacceptable risk to national security.

Subsection (b) requires a foreign adversary controlled application to provide any U.S. user with all available data related to their account provided by that application, upon request by the user, in a machine readable format, including any data maintained by the application regarding the user’s account, such as the user’s content and all other account information.

Subsection (c) provides the exemptions for the prohibition in subsection (a). It provides that the prohibition in subsection (a) does not apply to a foreign adversary controlled application regarding which a qualified divestiture is executed and shall cease to apply if a qualified divestment is executed after the effective date. This subsection also states that subsection (a) also does not apply to services provided with respect to a foreign adversary controlled application that are necessary for an entity to attain compliance with this Act.

Subsection (d) outlines the civil penalties for an entity found violating subsection (a) or subsection (b). An entity found violating subsection (a) shall be subject an amount not to exceed the amount that results from multiplying \$5,000 by the number of U.S. users determined to have accessed, maintained, or updated an application. An entity found violating subsection (b) shall be subject to a civil penalty in an amount not to exceed \$500 per U.S. user with an account provided by that application. This subsection also directs the Attorney General to conduct investigations related to potential violations of this Act and pursue enforcement if a violation has occurred.

Subsection (e) is a severability provision. 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. This subsection also clarifies that any invalidity of subsection (g)(3)(A) shall not affect or preclude the application from a determination as a foreign adversary controlled application under subsection (g)(3)(B).

Subsection (f) is a rule of construction stating that nothing in this Act may be construed to authorize the Attorney General to pursue enforcement other than what is specifically stated in this Act. It does not authorize the Attorney General to pursue enforcement against any individual user of the foreign adversary controlled application, nor does it alter or affect any other authority provided by or established under another provision of Federal law.

Subsection (g) defines key terms used throughout Section 2, including:

(1) The term “Controlled by a Foreign Adversary” means (A) a foreign person that is domiciled in, headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country; (B) an entity in which an entity or combination of entities identified in subparagraph (A), directly or indirectly owns a twenty percent stake or greater; or (C) an entity subject to the direction, or control, or of an entity identified in subparagraph (A) or (B).

(2) The term “Covered Company” means an entity that operates, directly or indirectly, including through its parent company, subsidiaries, or affiliates, a website, desktop application, mobile application, or augmented or immersive technology application that permits a user to create an account or profile to generate, share, and view text, images, videos, real-time communications, or similar content; has more than 1,000,000 monthly active users for a majority of months during the preceding 3 months the Presidential determination; enables one 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; and enables one or more users to view content generated by other users of the website, desktop application, mobile application, or augmented or immersive technology.

(3) The term does not include any website, desktop application, or mobile application in the United States whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.

(4) The term “Foreign Adversary Controlled Application” means a website, desktop application, mobile application, or augmented or immersive technology application is that is operated, directly or indirectly, including through its parent company, subsidiaries, or affiliates by:

(A) any of (i) ByteDance, Ltd.; (ii) TikTok; (iii) a subsidiary of or a successor to ByteDance, Ltd. or TikTok that is controlled by a foreign adversary; or (iv) a company owned or controlled directly or indirectly by such an entity; or

(B) a covered company that is controlled by a foreign adversary; and that is determined by the President to present a significant threat to the national security of the United States following the issuance of a public notice of the proposed presidential determination, a public report to Congress, to be submitted not less than 30 days prior to the presidential determination, describing the specific national security concern, which shall contain a classified annex, and describing what assets would need to be divested to be a qualified divestiture.

(5) The term “Foreign Adversary Country” means the countries identified pursuant to section 4872(d)(2) of title 10, United States Code (North Korea, People Republic of China, Russia, Iran).

(6) 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 one or more websites or online services, and which may include file hosting, domain name server hosting, cloud hosting, and virtual private server hosting.

(7) The term “Qualified Divestiture” means a divestiture or similar transaction that the President, through an interagency process, determines results in the foreign adversary controlled application no longer being controlled by a foreign adversary; and the President determines, through an interagency process, precludes the establishment or maintenance of any operational relationship between the foreign adversary controlled application’s United States operations after the date of the transaction and any formerly affiliated entities that are controlled by a foreign adversary, including, but not limited to, any cooperation with respect to the operation of a content recommendation algorithm or agreement with respect to data sharing.

(8) 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.

(9) The term “United States” means the “United States” including the territories of the United States.

### *Section 3. Judicial review*

This section requires any review challenging this Act to be filed only in the United States Court of Appeals for the District of Columbia Circuit. Subsection (b) provides that the United States Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over any challenge to this Act, or any action, finding, or determination under this Act. Subsection (c) places, upon enactment, a 165-day statute of limitation on any challenge

18

to this Act. This subsection also places a 90-day statute of limitations on any challenges to an action, finding, or determination under this Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

○





# Congressional Record

United States  
of America

PROCEEDINGS AND DEBATES OF THE 118<sup>th</sup> CONGRESS, SECOND SESSION

Vol. 170

WASHINGTON, MONDAY, APRIL 8, 2024

No. 59

## House of Representatives

The House was not in session today. Its next meeting will be held on Tuesday, April 9, 2024, at 12 p.m.

## Senate

MONDAY, APRIL 8, 2024

The Senate met at 3 p.m. and was called to order by the Honorable TAMMY DUCKWORTH, a Senator from the State of Illinois.

### PRAYER

The Chaplain, Dr. Barry C. Black, offered the following prayer:

Let us pray.

Precious Lord, we praise You with all our hearts because even when wrong seems to rule, you remain sovereign. You are our strength for today and our hope for tomorrow.

As our lawmakers open their hearts to You, may they sense that Your presence is as pervasive in statecraft as in religion. Illuminate their finite minds with Your eternal light, giving them wisdom beyond their own. Lord, remind our Senators that some problems You will not solve until they are ready to be used by You in working out the solutions.

We pray in your awesome Name. Amen.

### PLEDGE OF ALLEGIANCE

The Presiding Officer led the Pledge of Allegiance, as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

### APPOINTMENT OF ACTING PRESIDENT PRO TEMPORE

The PRESIDING OFFICER. The clerk will please read a communication

to the Senate from the President pro tempore (Mrs. MURRAY).

The legislative clerk read the following letter:

U.S. SENATE,  
PRESIDENT PRO TEMPORE,  
Washington, DC, April 8, 2024.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby appoint the Honorable TAMMY DUCKWORTH, a Senator from the State of Illinois, to perform the duties of the Chair.

PATTY MURRAY,  
President pro tempore.

Ms. DUCKWORTH thereupon assumed the Chair as Acting President pro tempore.

### RECOGNITION OF THE MAJORITY LEADER

The ACTING PRESIDENT pro tempore. The majority leader is recognized.

### MEASURES PLACED ON THE CALENDAR—S.J. RES. 67, S.J. RES. 68, S.J. RES. 69

Mr. SCHUMER. Madam President, I understand there are three joint resolutions at the desk due for a second reading en bloc.

The ACTING PRESIDENT pro tempore. The clerk will read the joint resolutions by title for the second time en bloc.

The legislative clerk read as follows:

A joint resolution (S.J. Res. 67) to provide for related procedures concerning the articles of impeachment against Alejandro Nicholas Mayorkas, Secretary of Homeland Security.

A joint resolution (S.J. Res. 68) providing for the issuance of a summons, providing for the appointment of a committee to receive and to report evidence, and establishing related procedures concerning the articles of impeachment against Alejandro Nicholas Mayorkas.

A joint resolution (S.J. Res. 69) to provide for related procedures concerning the articles of impeachment against Alejandro Nicholas Mayorkas, Secretary of Homeland Security.

Mr. SCHUMER. Madam President, in order to place the joint resolutions on the calendar under the provisions of rule XIV, I would object to further proceedings en bloc.

The PRESIDING OFFICER. Objection having been heard, the joint resolutions will be placed on the calendar.

### BUSINESS BEFORE THE SENATE

Mr. SCHUMER. Madam President, the Senate gavels back into session today to pick up right where we left off in March: confirming more of President Biden's outstanding nominees and advancing legislation that protects and serves the American people.

There is much the Senate has to accomplish in the coming weeks, and getting anything done—anything—will require bipartisan cooperation. It is not easy but nevertheless essential.

Today, the Senate will commence by voting to invoke cloture on the nomination of Susan Bazis to be a U.S. district court judge for the District of Nebraska. I have also filed cloture on the nominations of Robert White to be a district judge for the Eastern District of Maryland and the nomination of

• This "bullet" symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.



Printed on recycled paper.

S2629

JA 228

APP-48

judges of their choice to get a favorable outcome.

If courts like the Northern District of Texas refuse to adopt commonsense reforms to limit judge shopping, Congress should consider legislation to end this dangerous practice and restore trust in our Federal judiciary.

CHIPS AND SCIENCE

Mr. SCHUMER. Madam President, on Chips, well, this morning, another good announcement from President Biden. He and Commerce Secretary Raimondo announced the preliminary agreement with TSMC Arizona to provide billions in Chips and Science incentives to support more than \$65 billion in investments for three leading-edge fabs in Phoenix, AZ.

Just like the announcement of GlobalFoundries, Intel, and others, today's announcement proves Democrats are delivering in a big way on our promise to bring manufacturing back to the United States, to strengthen our national security, and to get ahead of rising costs from supply chain shortages. Today's announcement is precisely the kind of economic good news we have worked for for years in the Senate.

Five years ago, I approached my friend Senator YOUNG and told him we should work together on bipartisan legislation to boost U.S. investment and innovation in advanced manufacturing. I knew that if America wanted to remain No. 1 in terms of scientific might and industry, we had to get serious about getting the Federal Government to invest.

Thanks to the efforts of people like Senators KELLY and BROWN and CANTWELL and WYDEN and WARNER and many more, we passed Chips and Science into law, and we are now delivering these historic investments to power a new generation of American manufacturing. And there is yet more to come, with further investments in projects like Micron's proposed \$100 billion project in Upstate New York.

So I am thrilled to see that Chips and Science is delivering as intended and congratulate President Biden and Secretary Raimondo on this tremendous effort.

SOLAR ECLIPSE

Mr. SCHUMER. Madam President, finally, I have these glasses today, which were given to me by the president of Fordham University—special Fordham eclipse glasses—so now I am going outside to my balcony to take a look at the eclipse, which is reaching its peak at about 87 percent right now.

I yield the floor.

RESERVATION OF LEADER TIME

The ACTING PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

CONCLUSION OF MORNING BUSINESS

The ACTING PRESIDENT pro tempore. Morning business is closed.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

The ACTING PRESIDENT pro tempore. Under the previous order, the Senate will proceed to executive session to consider the following nomination, which the clerk will report.

The legislative clerk read the nomination of Susan M. Bazis, of Nebraska, to be United States District Judge for the District of Nebraska.

RECOGNITION OF THE MINORITY LEADER

The ACTING PRESIDENT pro tempore. The Republican leader is recognized.

NATIONAL SECURITY

Mr. MCCONNELL. Madam President, America's adversaries are working overtime to undermine our interests and erode the alliances that protect them.

And it is easy to concede that these challenges as playing out exclusively on the high seas of the Indo-Pacific or the borderlands of Europe or the Middle East. But in reality, the competition is not an "away game." America's greatest strategic rival is threatening our security right here on U.S. soil in tens of millions of American homes.

I am speaking, of course, of TikTok. Today, 170 million Americans are active users of the social media platform that the People's Republic of China treats as a tool of surveillance and propaganda.

TikTok officials like to insist that U.S. users' personal information, browsing histories, keystrokes, and other sensitive data are kept out of the reach of the PRC's teams of censors and propagandists. They claim that what it shows young Americans is what they want to see, not what the PRC wants them to think. But the company's own words shatter this fantasy:

Everything is seen in China.

That is the truth TikTok officials were willing to admit in a leaked recording from behind closed doors. And it shouldn't be all that surprising anyway: Chinese law requires that TikTok's Beijing-based parent company coordinate closely with the PRC.

All sorts of social media platforms can be fountains of disinformation and propaganda. Just look at last week's news about the PRC's efforts to manipulate Taiwan's elections with Twitter accounts driven by AI.

But with TikTok, we are not talking about meddling or hijacking an American platform. In this case, PRC influence and control has been baked in from the very beginning.

With Beijing's blessing, TikTok's algorithm pours gasoline on alarming trends from the glorification of Hamas terrorists to a particularly outrageous

fad that emerged last year where young people "discovered" the wisdom of Osama bin Laden.

I wish I was making this up. But let's be absolutely clear: This isn't a debate about restricting speech. After all, the PRC does enough of that itself. Chinese citizens are barred from accessing TikTok at all.

No matter how loudly TikTok's apologists claim that reining in PRC influence violates the First Amendment, the question we will face is about conduct, not content. I take a backseat to no one when it comes to protecting Americans' First Amendment rights. I have firmly defended American's right to even the most noxious forms of free speech like flag burning. But there is a serious difference between the views that Americans might express on TikTok and the actions taken by a platform that is beholden to our foremost strategic competitor.

Let me borrow an analogy from someone who has been relentless on this issue—FCC Commissioner Brendan Carr. Here is what he had to say:

You can use a pen to write salacious anti-American propaganda, and the government can't censor that content. Nor can it stop Americans from seeking such messages out. But if you use the same pen to pick a lock to steal somebody else's property, the government could prosecute you for illegal conduct.

The PRC has spent years trying to pick the lock of America's communications infrastructure, and the Federal Government has a long history of frustrating Beijing's efforts.

Requiring the divestment of Beijing-influenced entities from TikTok would land squarely within established constitutional precedent, and it would begin to turn back the tide of an enormous threat to America's children and to our Nation's prospects in defining the competition of the 21st century.

This is a matter that deserves Congress's urgent attention, and I will support commonsense, bipartisan steps to take one of Beijing's favorite tools of coercion and espionage off the table.

SUPPLEMENTAL GOVERNMENT FUNDING

Madam President, on a related matter, America's national security depends on sustained investment in both cutting-edge capabilities and expanded defense industrial capacity. That is why I continue to insist on overdue steps like the full-year Defense appropriations and national security supplemental the Senate passed earlier this year. As I have said repeatedly, outcompeting our top strategic adversary, the PRC, means projecting American strength far, far beyond the Indo-Pacific.

Beijing continues to menace Taiwan, the Philippines, and other Asian partners, but it is also conducting influence campaigns across the developing world and deepening its partnership with Moscow and Tehran.

Our closest and strongest allies in China's backyard understand this reality. Even as Japan deals with Chinese

maritime incursions and predatory trade practices at home, its leaders continue to remind us that the threats to Western prosperity and security are all connected.

Prime Minister Kishida, who will visit Washington this week and address a joint session of Congress, said just last week that “Russia’s aggression against Ukraine . . . shakes the foundation of the international order” and that “Japan will continue its cooperation [with] Ukraine.”

Critically, our ally’s words are backed up by actions. Over the past 2 years since Putin’s escalation, Japan has pledged \$12 billion to Ukraine’s resistance. Prime Minister Kishida’s trip to Kyiv last year made him the first Japanese leader to visit a conflict zone since World War II.

Just as importantly, Japan’s growing investments in its Self-Defense Force, including in cutting-edge capabilities like long-range strike—have made Japan an essential partner in deterring aggression in the Indo-Pacific.

Today, there is still room to work even more closely with committed allies like Japan to protect our technology from Chinese theft, leverage our advanced industries to improve collective security, and build more resilient supply chains.

More and more, America’s allies and partners—like the one we will welcome this week—understand both the gravity of the threats we face and the links between them. But, if America intends to remain the primary guarantor of our own security, we have to lead by example, and Congress has an opportunity to do that this week.

RYAN CORBETT

Now, Madam President, on another matter, the disastrous consequences of America’s withdrawal from Afghanistan were both foreseeable and foreseen, and as Taliban rule terrorizes the region and brutalizes the Afghan people, it has also inflicted terrible pain on American families.

I have worked closely with the family of Ryan Corbett, an American citizen detained in Afghanistan by the Taliban.

For over a decade, prior to the fall of Kabul, Ryan and his family lived amongst the Afghan people, where they served the community and ran a business focused on providing Afghans with education and training to start their own businesses. As the Taliban returned to power, the Corbett family was forced to flee, but Ryan made the difficult decision to return, hoping to pay his staff and keep his business afloat. And, on August 10, 2022, the Taliban detained him without charge.

For 607 days, Ryan has been confined to a 9-by-9 basement cell, with scraps for food, little to no sunlight, and intermittent contact with his family. After nearly 2 years of wrongful detention, his hopes of ever returning to America are dimming.

Earlier this afternoon, I had a chance to meet with Ryan’s wife, Anna, their

three teenaged children, and his parents, Drue and Evelyn, from Louisville. Now, more than ever, they fear for Ryan’s life.

Today, the Democratic leader and I have introduced a resolution calling for Ryan’s immediate release. It reaffirms America’s commitment to freeing Ryan and raising the international stakes of the Taliban’s wrongful detention of American citizens.

Unfortunately, while Ryan languishes in captivity, the Biden administration sends a different message to his captors. Since his detention, the U.S. Government has sent roughly \$1 billion in aid to a country in the tight grip of a medieval, theocratic regime.

It is time to put the Taliban’s violent rule on notice. It is time to show our enemies that the United States will not let American citizens be used as bargaining chips. It is time to bring Ryan Corbett home.

The ACTING PRESIDENT pro tempore. The senior Senator from Illinois.

WORLD CENTRAL KITCHEN

Mr. DURBIN. Madam President, last week, we saw another tragedy in Gaza—an attack that killed seven people delivering desperately needed, life-saving humanitarian aid. The victims were employees of the World Central Kitchen, an amazing organization run by an extraordinary individual, Jose Andres.

They started to feed people in Haiti after the 2010 earthquake, and they have continued their mission in some of the most challenging parts of the world. Andres’ innovative and courageous team has been helping people in Gaza since the crisis began in October, providing critical food to millions of innocents caught in the conflict.

I joined Mr. Andres in a meeting in our Capitol just a few weeks ago with a few other Senators. He told us of his ambitious plans to increase food aid to Gaza.

I have always admired his ingenuity and tenacity in taking on these truly lifesaving operations for those most in need. Mr. Andres is truly a hero. So my heart goes out to him and the families of those on his team who were recklessly and avoidably killed last week, adding to the more than 200 aid workers who have been killed in Gaza.

We have seen a series of seemingly cascading crises in this conflict, and the list keeps growing: October 7, the Hamas attack on Israel that killed 1,200 and took more than 200 people hostage; the widespread destruction and loss of civilian life and growing humanitarian crisis in Gaza amid Israel’s response that lacks any long-term strategy and is made worse by Hamas’s hiding among civilians; the continued holding of Israeli hostages, including one with ties to our home State of Illinois, by Hamas and Hamas’s refusal to accept a ceasefire in exchange for their release; the bewildering and inexcusable failure of Israel to set up deconfliction mechanisms for adequate aid delivery; and the failure to recog-

nize that a massive military-only response by Israel will never provide a long-term path to stability and end the cycle of violence.

I have long said that I do not think the current Israeli or Palestinian leadership is really up to the challenge needed to bring hope, stability, or a viable two-state solution to the region. Early in the conflict, I cautioned the Israelis not to be blinded by their pain from October 7 and make the same types of mistakes we made after September 11—a warning I believe the current leadership in Israel has failed to heed.

But, if unable to learn from our missteps, then perhaps they should listen to former Mossad Chief Meir Dagan, who, before his death years ago, concluded that Israel, over the decades, “achieved a long string of impressive tactical successes but also disastrous strategic failures.” Tragically, I am worried that that is the same case today.

Chef Andres has made a similar point with which I agree—that Israel’s strategy in Gaza is futile and indefensible with so much innocent loss of human life.

I have long called for a ceasefire that includes the release of the remaining hostages as well as a sustained, U.S.-led Gaza relief operation that includes food, medicine, and other critical basics. The inexcusable deaths of the World Central Kitchen staff in Gaza are reminders that these steps are needed now more than ever.

(The remarks of Mr. DURBIN pertaining to the introduction of S. Res. 629 are printed in today’s RECORD under “Statements on Introduced Bills and Joint Resolutions.”)

Mr. DURBIN. I yield the floor.

I suggest the absence of a quorum.

The ACTING PRESIDENT pro tempore. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. CORNYN. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

MAYORKAS IMPEACHMENT

Mr. CORNYN. Madam President, as we all know, 2 months ago, the House of Representatives impeached Homeland Security Secretary Alejandro Mayorkas, who has led the Department of Homeland Security since the beginning of the Biden administration.

For 3 years, Secretary Mayorkas has overseen the record-breaking crisis at the southern border. During that time, Customs and Border Protection have logged more than 7.4 million migrant encounters—more than two previous administrations combined—and that was over a period of 12 years. In 3 years, the Biden administration has accomplished what took 12 years for the Obama and Trump administrations.

Law enforcement’s focused response on migrant crossings has caused security missions, including drug interdiction, to take a hit. Staffing shortages



# Congressional Record

United States  
of America

PROCEEDINGS AND DEBATES OF THE 118<sup>th</sup> CONGRESS, SECOND SESSION

Vol. 170

WASHINGTON, TUESDAY, APRIL 23, 2024

No. 71

## Senate

The Senate met at 10 a.m. and was called to order by the Honorable RAPHAEL G. WARNOCK, a Senator from the State of Georgia.

### PRAYER

The Chaplain, Dr. Barry C. Black, offered the following prayer:

Let us pray.

O Lord, our Redeemer, abide with our Senators through the passing hours of another day. Strengthen them to stand firm for those good and eternal values that keep a nation strong. Lord, give them the courage to do the right even when others are doing wrong. Remind them that You are the pilot of their lives who can guide them to a desired destination. Let discretion preserve them, understanding keep them, and faith fortify them. Lead them not into temptation, but deliver them from the forces of evil. Save them from pride that mistakes their abilities for possessions, and keep them humble enough to see their need of You.

We pray in Your Holy Name. Amen.

### PLEDGE OF ALLEGIANCE

The Presiding Officer led the Pledge of Allegiance, as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

### APPOINTMENT OF ACTING PRESIDENT PRO TEMPORE

The PRESIDING OFFICER. The clerk will please read a communication to the Senate from the President pro tempore (Mrs. MURRAY).

The senior assistant legislative clerk read the following letter:

U.S. SENATE,  
PRESIDENT PRO TEMPORE,  
Washington, DC, April 23, 2024.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby

appoint the Honorable RAPHAEL G. WARNOCK, a Senator from the State of Georgia, to perform the duties of the Chair.

PATTY MURRAY,  
President pro tempore.

Mr. WARNOCK thereupon assumed the Chair as Acting President pro tempore.

### RESERVATION OF LEADER TIME

The ACTING PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

### CONCLUSION OF MORNING BUSINESS

The ACTING PRESIDENT pro tempore. Morning business is closed.

### LEGISLATIVE SESSION

#### SECURING GROWTH AND ROBUST LEADERSHIP IN AMERICAN AVIATION ACT—MOTION TO PROCEED—Resumed

The ACTING PRESIDENT pro tempore. Under the previous order, the Senate will resume consideration of the motion to proceed to H.R. 3935, which the clerk will report.

The senior assistant legislative clerk read as follows:

Motion to proceed to Calendar No. 211, H.R. 3935, a bill to amend title 49, United States Code, to reauthorize and improve the Federal Aviation Administration and other civil aviation programs, and for other purposes.

#### RECOGNITION OF THE MAJORITY LEADER

The ACTING PRESIDENT pro tempore. The majority leader is recognized.

#### NATIONAL SECURITY ACT, 2024

Mr. SCHUMER. Mr. President, it is my understanding that the Senate has received a message from the House of

Representatives to accompany H.R. 815.

The ACTING PRESIDENT pro tempore. The Senator is correct.

Mr. SCHUMER. I ask that the Chair lay before the Senate the message to accompany H.R. 815.

The ACTING PRESIDENT pro tempore. The Chair lays before the Senate a message from the House.

The senior assistant legislative clerk read as follows:

Resolved, That the House agree to the amendment of the Senate to the bill (H.R. 815) entitled "An Act to amend title 38, United States Code, to make certain improvements relating to the eligibility of veterans to receive reimbursement for emergency treatment furnished through the Veterans Community Care program, and for other purposes.", with a House amendment to the Senate amendment.

#### MOTION TO CONCUR

Mr. SCHUMER. I move to concur in the House amendment to the Senate amendment to H.R. 815, and I ask for the yeas and nays.

The ACTING PRESIDENT pro tempore. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays are ordered.

#### CLOTURE MOTION

Mr. SCHUMER. Mr. President, I send a cloture motion to the desk.

The ACTING PRESIDENT pro tempore. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The senior assistant legislative clerk read as follows:

#### CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, do hereby move to bring to a close debate on the motion to concur in the House amendment to the Senate amendment to H.R. 815, a bill to amend title 38, United States Code, to make certain improvements relating to the eligibility of veterans to receive reimbursement for emergency treatment furnished through the Veterans Community Care program, and for other purposes.

• This "bullet" symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.



Printed on recycled paper.

S2943

JA 231

APP-98

about business when foreign adversaries weaponize data, weaponize technology, and weaponize business approaches that hurt Americans.

I want to yield to my colleague, the chairman of the Senate Intelligence Committee, for his perspective on why this legislation before us is so important.

The PRESIDING OFFICER. The Senator from Virginia.

Mr. WARNER. Mr. President, first of all, I want to agree with my friend, the chairman of the Commerce Committee, on issues she already outlined, whether it be the need for aid for Ukraine, support for Israel, humanitarian aid for Gaza, or the necessary funding that has taken place for the Indo-Pacific, and, obviously, legislation that we all supported on fending off fentanyl.

But I want to particularly commend her for comments she has made on these technology issues. Over the last 7 years, as vice chair and now chairman of the Intelligence Committee, I spent an awful lot of time looking at what I think is one of the most significant intelligence failures of the last half century, and that was the failure we had to anticipate and disrupt Russian efforts to meddle in our elections. Since that time, though, we have seen a wide spectrum of foreign adversaries who tried to copy the Russian playbook.

But don't just take it from me. A succession of now-declassified intelligence assessments has described the ways in which foreign adversaries like Iran, like the People's Republic of China, and others are seeking to stoke social, racial, and political tensions in the United States. They are seeking to undermine confidence in our institutions and our elections systems and even to sow violence amongst Americans. The extent to which our adversaries have exploited American social media platforms is a matter of public record.

The committee I chair has held many hearings—open hearings—on the failure of U.S. social media platforms to identify the exploitation of their products by foreign intelligence services. As a Senator, along with the Senator from Washington, I have been among the leading critics of these platforms for their repeated failures to protect consumers.

While the exploitation of U.S. communication platforms by adversaries continues to be a serious issue, at the end of the day, our platforms are at least independent businesses. They do not have a vested interest in undermining our basic democratic system.

The truth is, though, I can't say the same for TikTok, the fastest growing social media platform in the United States, whose parent company ByteDance is based in the PRC. Even as U.S. social media platforms have fumbled in their response to foreign influence operations, there was never any concern that these platforms would operate at the direction of a foreign adversary. Again, I cannot say the same for TikTok.

I yield back to Senator CANTWELL.

The PRESIDING OFFICER. The Senator from Washington.

Ms. CANTWELL. I thank Senator WARNER for his perspective as chairman of the Intelligence Committee and his hard work. He and I both drafted legislation more than a year ago trying to give our government the tools to deal with this issue.

In 2020, India concluded that TikTok and other Chinese-controlled apps were national security threats and prohibited them. As a result, India TikTok users migrated to other platforms, including Google's YouTube, and Indian small businesses found other ways to operate on other platforms.

This supplemental contains the Protecting Americans from Foreign Adversary Controlled Applications Act. Congress has a nonpunitive policy purpose in passing this legislation. Congress is not acting to punish ByteDance, TikTok, or any other individual company. Congress is acting to prevent foreign adversaries from conducting espionage, surveillance, and malign operations harming vulnerable Americans, our servicemen and women, and our U.S. Government personnel.

The PRESIDING OFFICER. The Senator from Virginia.

Mr. WARNER. I would like to expound a little bit on what Senator CANTWELL just said. It has been made absolutely clear that a number of Chinese laws require Chinese companies and their subsidiaries to assist PRC security agencies and abide by the secret and unchallengeable government directives. The truth is, these Chinese companies, at the end of the day, don't owe their obligation to their customers or their shareholders, but they owe it to the PRC Government.

In the context of social media platforms used by nearly half of Americans, it is not hard to imagine how a platform that facilitates so much commerce, political discourse, and social debate could be covertly manipulated to serve the goals of an authoritarian regime, one with a long track record of censorship, transnational oppression, and promotion of disinformation.

In recent weeks, we have seen direct lobbying by the Chinese Government, indicating, perhaps, more than anything we will say on the floor here, how dearly Xi Jinping is invested in this product—a product, by the way, that is not even allowed to operate in the Chinese domestic market, itself.

Story after story, over the last 18 months, have exposed the extent to which TikTok had grossly misrepresented its data security and corporate governance practice, as well as its relationship with its parent company. Countless stories have refuted the claims made by TikTok executives and lobbyists that it operates independently from its controlling company ByteDance.

We have also seen documented examples of this company surveilling journalists. We have seen corresponding

guidance from leading news organizations, not just here in America but across the world, advising their investigative journalists not to use TikTok. These public reports, based on revelations of current and former employees, also reveal that TikTok has allowed employees to covertly amplify content.

Unfortunately, those who suggest that the United States can address the data security and foreign influence risk of TikTok through traditional mitigation have not been following TikTok's long track record of deceit and lack of transparency.

I yield back to Senator CANTWELL.

Ms. CANTWELL. I thank Senator WARNER for his comments.

I find it most disturbing that they used TikTok to repeatedly access U.S. user data and track multiple journalists covering the company. Researchers have found that TikTok restricts the information that Americans and others receive on a global basis.

As of December 2023, an analysis by Rutgers University found that TikTok posts mentioning topics that are sensitive to the Chinese Government, including Tiananmen Square, Uighurs, and the Dalai Lama were significantly less prevalent on TikTok than on Instagram, the most comparable social media.

Foreign policy issues disfavored by China and Russian Governments also had fewer hashtags on TikTok, such as pro-Ukraine or pro-Israel hashtags. Here are some of those hashtags on TikTok:

The example of Tiananmen Square, which we all know was an example of students standing up to the military, and yet for Tiananmen Square, there are 8,000 percent more hashtags on Instagram than on TikTok.

The Uighur genocide protecting a Muslim population, there are 1,970 percent more hashtags about that on Instagram than on TikTok.

And my personal favorite, just because I had the privilege of meeting the Dalai Lama here in the Capitol, 5,520 percent more hashtags where the Dalai Lama is mentioned on Instagram than on TikTok.

And pro-Ukraine, 750 percent more hashtags on Instagram than on TikTok about Ukraine and support for Ukraine.

I think that says it all in this debate today. Are we going to continue to allow people to control the information by using an export-controlled algorithm and China-based source code?

My colleagues and I are urging for this deweaponization by saying that TikTok should be sold. Now, I know that the Chinese have an export control on that algorithm. Congress believes that you have to have adequate time to sufficiently address this issue posed by our foreign adversaries. That is why the legislation before us is for ByteDance to sell its stake in TikTok.

We think a year is ample time to allow potential investors to come forward, for due diligence to be completed, and for lawyers to draw up and

finalize contracts. This is not a new concept to require Chinese divestment from U.S. companies.

The Committee on Foreign Investment in the United States requires Chinese divestment from hotel management platforms—StayNTouch, from a healthcare app called PatientsLikeMe, from the popular LGBTQI dating app Grindr, among other companies. And even after the Chinese owner divested from Grindr in 2020, Americans had continuity of service on this platform.

So I turn it back to my colleague, but we are giving people a choice here to improve this platform and have the opportunity for Americans to make sure that they are not being manipulated by our foreign adversaries.

Mr. President, I ask unanimous consent that H. Res. 1051, the House resolution originally on this legislation, be printed in the RECORD.

There being no objection, the material as ordered to be printed in the RECORD, as follows:

H. RES. 1051

Whereas TikTok collects vast amounts of data on Americans, though the total extent of its collection is unknown:

(1) On August 6, 2020, the President concluded that TikTok “automatically captures vast swaths of information from its users” and that TikTok’s ownership by ByteDance Ltd. enables the People’s Republic of China (referred to in this resolution as the “PRC”) and Communist Party of China (referred to in this resolution as the “CCP”) to gain access to “Americans’ personal and proprietary information,” potentially allowing the CCP “to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage”.

(2) Outside reporting has confirmed the breadth of TikTok’s reach, concluding that its data collection practices extend to age, phone number, precise location, internet address, device used, phone contacts, social network connections, content of private messages sent through the application, and videos watched.

(3) On November 11, 2022, Federal Communications Commissioner Brendan Carr explained that “underneath [TikTok], it operates as a very sophisticated surveillance app.” He characterized it as “a big risk” for multiple reasons, including espionage. The risk posed by TikTok is exacerbated by the difficulty in assessing precisely which categories of data it collects. For example, outside researchers have found embedded vulnerabilities that allow the company to collect more data than the application’s privacy policy indicates.

Whereas PRC law requires obligatory, secret disclosure of data controlled by Chinese companies at the PRC’s unilateral request:

(1) Pursuant to PRC law, the PRC can require a company headquartered in the PRC to surrender all its data to the PRC, making it an espionage tool of the CCP.

(2) The National Intelligence Law, passed in China in 2017, states that “any organization” must assist or cooperate with CCP intelligence work. Such assistance or cooperation must also remain secret at the PRC’s request.

(3) The PRC’s 2014 Counter-Espionage Law states that “relevant organizations . . . may not refuse” to collect evidence for an investigation.

(4) The PRC’s Data Security Law of 2021 states that the PRC has the power to access and control private data.

(5) The PRC’s Counter-Espionage Law grants PRC security agencies nearly unfettered discretion, if acting under an effectively limitless capacious understanding of national security, to access data from companies.

(6) On September 17, 2020, the Department of Commerce concluded that the PRC, to advance “its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment,” is constructing “massive databases of Americans’ personal information” and that ByteDance has close ties to the CCP, including a cooperation agreement with a security agency and over 130 CCP members in management positions.

(7) On December 2, 2022, the Director of the Federal Bureau of Investigation, Christopher Wray, stated that TikTok’s data repositories on Americans “are in the hands of a government that doesn’t share our values and that has a mission that’s very much at odds with what’s in the best interests of the United States. . . . The [CCP] has shown a willingness to steal Americans data on a scale that dwarfs any other”.

(8) On December 5, 2022, the Director of National Intelligence, Avril Haines, stated, when asked about TikTok and PRC ownership, “It is extraordinary the degree to which [the PRC] . . . [is] developing frameworks for collecting foreign data and pulling it in, and their capacity to then turn that around and use it to target audiences for information campaigns and other things, but also to have it for the future so that they can use it for a variety of means”.

(9) On December 16, 2022, the Director of the Central Intelligence Agency, William Burns, explained that “because the parent company of TikTok is a [PRC] company, the [CCP] is able to insist upon extracting the private data of a lot of TikTok users in this country, and also to shape the content of what goes on to TikTok as well to suit the interests of the Chinese leadership”.

(10) On August 2, 2020, then-Secretary of State, Mike Pompeo, stated that PRC-based companies “are feeding data directly to the Chinese Communist Party, their national security apparatus”.

(11) Public reporting has repeatedly confirmed statements made by the Executive Branch regarding the tight interlinkages between ByteDance, TikTok, and the CCP.

(A) The Secretary of ByteDance’s CCP committee, Zhang Fuping, also serves as ByteDance’s Editor-in-Chief and Vice President and has vowed that the CCP committee would “take the lead” across “all product lines and business lines”, which include TikTok.

(B) On May 30, 2023, public reporting revealed that TikTok has stored sensitive financial information, including the Social Security numbers and tax identifications of TikTok influencers and United States small businesses, on servers in China accessible by ByteDance employees.

(C) On December 22, 2022, public reporting revealed that ByteDance employees accessed TikTok user data and IP addresses to monitor the physical locations of specific United States citizens.

(D) On June 17, 2022, public reporting revealed that, according to leaked audio from more than 80 internal TikTok meetings, China-based employees of ByteDance repeatedly accessed nonpublic data about United States TikTok users, including the physical locations of specific United States citizens.

(E) On January 20, 2023, public reporting revealed that TikTok and ByteDance employees regularly engage in practice called “heating,” which is a manual push to ensure specific videos “achieve a certain number of video views”.

(F) In a court filing in June 2023, a former employee of ByteDance alleged that the CCP spied on pro-democracy protestors in Hong Kong in 2018 by using backdoor access to TikTok to identify and monitor activists’ locations and communications.

(G) On November 1, 2023, public reporting revealed that TikTok’s internal platform, which houses its most sensitive information, was inspected in person by CCP cybersecurity agents in the lead-up to the CCP’s 20th National Congress.

Whereas the PRC’s access to American users’ data poses unacceptable risks to United States national security:

(1) As a general matter, foreign adversary controlled social media applications present a clear threat to the national security of the United States.

(2) The Department of Homeland Security has warned that the PRC’s data collection activities in particular have resulted in “numerous risks to U.S. businesses and customers, including: the theft of trade secrets, of intellectual property, and of other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service; security and privacy risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses”. These risks are imminent and other, unforeseen risks may also exist.

(3) On September 28, 2023, the Department of State’s Global Engagement Center issued a report that found that “TikTok creates opportunities for PRC global censorship”. The report stated that United States Government information as of late 2020 showed that “ByteDance maintained a regularly updated internal list identifying people who were likely blocked or restricted from all ByteDance platforms, including TikTok, for reasons such as advocating for Uyghur independence”.

(4) On November 15, 2022, the Director of the Federal Bureau of Investigation, Christopher Wray, testified before the Committee on Homeland Security of the House of Representatives that TikTok’s national security concerns “include the possibility that the [CCP] could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so choose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices”.

(5) On March 8, 2023, the Director of the Federal Bureau of Investigation, Christopher Wray, testified before the Select Committee on Intelligence of the Senate that the CCP, through its ownership of ByteDance, could use TikTok to collect and control users’ data and drive divisive narratives internationally.

Whereas Congress has extensively investigated whether TikTok poses a national security threat because it is owned by ByteDance:

(1) On October 26, 2021, during the testimony of Michael Beckerman, TikTok head of public policy for the Americas, before a hearing of the Subcommittee on Consumer Protection of the Committee on Commerce, Science, and Transportation of the Senate, lawmakers expressed concerns that TikTok’s audio and user location data could be used by the CCP.

(2) On September 14, 2022, lawmakers expressed concerns over TikTok’s algorithm and content recommendations posing a national security threat during a hearing before the Committee on Homeland Security and Governmental Affairs of the Senate with Vanessa Pappas, Chief Operating Officer of TikTok.

our most prestigious universities, their campuses are closed because they have been taken over by pro-terrorist mobs, chanting things and harassing Jewish students to go back to Poland, they say. Others are chanting: "Go Hamas. We love you. We support your rockets too." Others—I have heard these chants—here it goes: "We say justice. You say how. Burn Tel Aviv to the ground."

The situation has gotten so intolerable that, just 2 days ago, a rabbi advised Jewish students to leave Columbia University and go home for their safety.

This morning, I got a text message from a friend—a Jewish friend—and I read something I never thought I would ever have to read. Here is what he wrote me:

I have to tell you, for the first time in my life, I see Jewish people scared for their safety and considering exit strategies from the USA, including buying homes in foreign countries and looking to liquidate USA assets.

I never thought I would ever read that from anybody in America.

These mobs, by the way, don't just want to destroy Israel. They want to destroy America. Some of these mobs are out there chanting "death to America" in the streets of American cities.

As for one of the mob leaders at one of these riots, this is what he said into a microphone:

It is not just "Genocide Joe" that has to go; it is the entire system that has to go. Any system that would allow such atrocities and devility to happen and would support it—such a system does not deserve to exist on God's Earth.

Do you know what system he is talking about? This system—our system, our system of government—that is what he was talking about.

Where did all of this come from? How did all of this happen from one day to the next? How can things that we once only saw happening in the streets of Tehran, manufactured by the evil regime—how are those things now being chanted in our streets in our country? Where did this come from? The clues are everywhere.

Hamas and Hezbollah have been very, very public about how these violent, anti-Israel, anti-Semitic mobs are part of their strategy to intimidate American leaders to support policies that will help destroy Israel.

Hamas, Hezbollah, and other terror groups have repeatedly called on their supporters around the world to protest "in cities everywhere," and they boast about how their friends—or who they call their "friends on the global left"—were actually now responding to their calls.

By the way, they openly brag. This is all coming from interviews that they do on television programs that can be monitored. They openly brag that this is "because of the introduction of colonialism, racism, and slavery studies into history curricula."

They go on to say that many young Americans have been—this is my term,

a term I read today in the Wall Street Journal—have been groomed to "support armed resistance," to support intifada in the United States.

By the way, it is not just the mobs that we are seeing. Beyond that, as the Director of the FBI has acknowledged, ISIS generates income—they generate revenue—by running a human smuggling ring that brings migrants to the United States.

Just the bare minimum common sense would lead you to conclude that, if ISIS has a business to smuggle migrants into the United States, why wouldn't they use that to smuggle a few terrorists here to do in America what they did in Moscow a few weeks ago?

So we have Hamas, and we have Hezbollah, and we have all of these terror groups encouraging and supporting violent mobs calling for intifada inside America. We already have people here, on student visas, calling for "Death to America," and ISIS controls a migrant smuggling ring that they can use to bring people into the United States to conduct attacks.

But if I want to help Israel, if I want to help Taiwan, if I want to help Ukraine, if I want to ban TikTok, I have to agree; I have to vote to do nothing to stop thousands of people a day whom we know literally nothing about—just allow them to come across our border and be released into our country.

As far as some of the money that is being spent all over the world, I have always supported the United States being engaged in the world, and I continue to be, but I ask you this: I have senior citizens, and I have veterans, and they call my office, and they call our offices, and they say: I have nowhere to live. Housing is too expensive.

I met a senior, a couple of days ago, in his eighties. He still has to work nights as a security guard, and he literally lives in a mobile home—not even a mobile home, in like a trailer parked in someone's backyard.

These people call. They have lived in this country their whole lives. They have served our country. They call for help, and the most we can often do is help get them on a waiting list for section 8 housing. This is a problem that exists in America right now.

But if I want to help Israel, if I want to help Taiwan, if I want to help Ukraine, if I want to ban TikTok, I have to vote for spending billions of dollars to give to charity groups so they can fly people around the country here and put them up in hotel rooms or so they can help for resettlement in another country.

We have rich countries in the Middle East, allies of ours. Their leaders own some of the largest yachts in the world. Some of their leaders own some of the most expensive horses you could possibly buy in the world. They have built some of the most extravagant and luxurious resorts on the planet in some of these countries. These are rich coun-

tries and strong supporters of the Palestinian cause, as they call it.

But if I want to help Israel, if I want to help Taiwan, if I want to help Ukraine, if I want to ban TikTok, I have to vote to send American taxpayer money to deal with the catastrophe that has been created by Hamas in Gaza—100 percent by Hamas. There was no war. There was a ceasefire before Hamas crossed over and slaughtered and raped and kidnapped. But now the American taxpayer is on the hook.

Look, I understand that, in our Republic, in our system of government, compromise is necessary. We have to do it all the time. I have passed a lot of bills—I am very proud of that—and every one of them involved my finding someone from a different ideological perspective, from the other side of the aisle. You have to compromise, meaning you are not going to get everything you want. You are going to have to give them something they want in exchange for something you want or you may have to change the way you wrote what you want. That is what you have to do in order to pass laws.

I understand compromise—I do—but this bill is not that. This bill is not a compromise. This bill is basically saying that, if I don't agree to drop my demands that the President secure our border, if I don't agree to spend billions of taxpayer dollars all over the world to resettle people here and in other places in the midst of our own migratory crisis—if I don't agree to all of that, then Israel and Taiwan and Ukraine do not get the help they need and that I support, and TikTok does not get banned. This is not compromise. This is legislative blackmail, and I will not vote for blackmail.

I yield the floor.

The PRESIDING OFFICER. The Senator from Nebraska.

Mr. RICKETTS. Mr. President, does anybody believe that hashtag "StandwithKashmir" is organically more popular than hashtag "TaylorSwift"? No, of course not, but right now, on TikTok, hashtag "StandwithKashmir" has 20 times more posts than hashtag "TaylorSwift."

This is a direct example of the Chinese Communist Party using their control of TikTok to skew public opinion on foreign events in their favor. China is our chief foreign adversary in the world. They are a threat to our national security, our values, our economy, and the CCP works tirelessly every day to undermine our entire way of life. TikTok is one of the ways they are doing that.

I understood that as Governor. That is why I was the first Governor in the country to ban the use of TikTok on State devices back in 2020, and that is why I will be voting for this bill today. Today, we are taking action to end the Chinese Communist Party's ability to own and operate TikTok in the United States.

TikTok's active users include over 150 million Americans. That is almost half of our country's entire population. It has become the most influential news platform in the country. The percentage of TikTok users who regularly get their news from this app has doubled since 2020. The problem, however, is that what that news is, what slant that news has, is being entirely controlled by the Chinese Communist Party. We don't allow this for TV stations or radio stations. You have to be a U.S. citizen to own a TV station or a radio station in this country. Why are we letting our greatest adversary in the world own a news platform?

TikTok, under CCP ownership, promotes or demotes content based on whether it aligns with the CCP's interests and its agenda. This has major, real-world implications here at home and around the world.

Look at what is happening on our college campuses right now in this country. Pro-Hamas activists are taking over public spaces and making it impossible for campuses to operate. Jewish students are being told to leave campus because their universities can't guarantee their safety. There are a lot of other things wrong with this, including the failure to prioritize student safety over appeasement of terrorist sympathizers.

But why is this happening?

Well, let's look at where young people are getting their news. Nearly a third of adults 18 to 29 years old—these young people in the United States—are regularly getting their news exclusively from TikTok. Pro-Palestinian and pro-Hamas hashtags are generating 50 times the views on TikTok right now despite the fact that polling shows Americans overwhelmingly support Israel over Hamas. These videos have more reach than the top 10 news websites combined.

This is not a coincidence. The Chinese Communist Party is doing this on purpose. They are pushing this racist agenda with the intention of undermining our democratic values, and if you look at what is happening at Columbia University and other campuses across the country right now, they are winning.

I want to talk about another example that means a lot to folks back home whom I represent in Nebraska.

We know that the COVID-19 pandemic originated in China. Instagram and TikTok currently have about the same number of users in the United States; However, if you look at the content, there is a 400-to-1 ratio for content that blames China for this pandemic on Instagram compared to TikTok. Again, Instagram has 400 times the number of posts blaming China for COVID than on TikTok.

On TikTok, the Chinese Communist Party has quashed dissent or criticism. They have done this for Tiananmen Square—which, again, on Instagram, there are 80 times the posts around Tiananmen Square than there are on

TikTok, and on Hong Kong, there are 180 times the posts on Hong Kong being censored or being repressed versus on TikTok.

The Federal Government's job is to protect Americans against foreign and domestic threats. TikTok is a major foreign threat. The bill we are passing today puts an end to that. This bill ensures that our citizens are not improperly targeted, surveilled, or influenced by any foreign adversary.

Right now, the major threat is TikTok, but China can make another TikTok. That is why, instead of going after any specific app, this bill simply prohibits marketplaces, like the App Store or Google Play, from hosting applications controlled by foreign adversaries. This is just common sense.

It also establishes a narrow framework to protect against future apps. It allows the Federal Government to require divestment of applications controlled by a foreign adversary or face a prohibition on app stores and be denied access to web-hosting services in the United States. That power has very strict guidelines. The authority can only be exercised if an application is under the control of an adversarial foreign entity, presents a national security threat, and has over 1 million active users annually.

It also protects individual users. No enforcement action can be taken against individual users of banned applications. Civil enforcement actions may only be initiated against companies that violate the act.

The bill incentivizes China to divest from TikTok or TikTok will face a ban. If TikTok is divested from the CCP, it can continue to operate in the United States. If the restrictions are already in effect and TikTok is divested later, the restrictions will be lifted.

I believe the Chinese Communist Party is the greatest threat we face in this Nation. They are fighting smart, trying to undermine us from within, and using technology like TikTok to do it. Together, by passing this bill, it is my hope that we will send a loud message and a clear message that America is not open to the CCP for influence.

We are taking a stand to protect our own, protect our values, and end a major Communist Chinese Party tool to attack us.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. Mr. President, long before I ever thought of running for office, I was a little kid born in a West Virginia coal mining town called Beckley. My sister and I ended up going to the same grade school not too far from our house.

As a kid, I was pretty well behaved and didn't get into much trouble, but in the first grade, I got in a fight. I got in a fight because some kid was picking on my sister, who was a year older, in the second grade. He was a much bigger

guy, and it was not a fair fight. I got involved in it and took him out with one swing. That was the last punch that I think I had thrown in anger. But I didn't like the idea of a big guy, a bully, trying to push around somebody, whether it was my sister or not. I have never cared for that in other situations growing up and watching the behavior of people in all kinds of different situations.

Our country, if you go back to our founding, if you recall, we took on the biggest nation on Earth, the strongest nation on Earth, Great Britain. It was not a fair fight. They had us badly outgunned, outnumbered. And somebody came to our rescue. The persons who came to our rescue were the French. If it weren't for the French, we would still be, maybe, a colony of Great Britain. But the French stood up and said: We are here to help.

There is a time for people to stand—countries to stand by and allow things to happen, and there is a time to stand up and be heard. We were helped as a nation over 200 years ago by the French. We have, I think, a moral obligation to help make sure that Ukraine has an opportunity to continue to go forward and to be a democratic nation. They are a democratic nation. They actually choose—they elect their own leaders. Vladimir Putin doesn't care very much for that. He thinks they shouldn't be allowed to do so and has decided to use force to be able to take away the opportunity to be a free nation.

We have a couple of opportunities. We can criticize Putin, the Russians, for what they are doing or we can actually do something about it.

I think I may be the last Vietnam veteran serving here in the U.S. Senate. When we go out from here, I like to run. Many, many mornings when I have gone for a run near the Capitol, I have run out to the Lincoln Memorial. On my way back, I run right by the Vietnam Memorial. It is black granite. There are names of I want to say maybe 59,000 people who died in that war I served in.

We got involved in that war. It was not a popular war. It wasn't popular with my generation. But we got involved in that war. The communists in North Vietnam were coming in and trying to take over the south. We ended up, for better or for worse, aligning with the south. We know what the outcome turned out to be. A lot of people died. A lot of people died in that war. I know a number of them, and my guess is my colleagues do as well.

I tell that story because we have a situation here that is not altogether different in which the Ukrainian people, who want to defend themselves—they want to preserve their democracy, and they are willing to make the tough fight if we will help them and the rest of the free world will help them.

God bless our President and leaders of a bunch of other countries who said: We are not going to walk away and let



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

**DRAFT NATIONAL SECURITY AGREEMENT**

This NATIONAL SECURITY AGREEMENT (“**Agreement**”) is made as of [date] (the “**Effective Date**”), by and among: (i) ByteDance Ltd., a Cayman Islands exempted company (“**ByteDance**”); (ii) TikTok Ltd., a Cayman Islands exempted company (“**TikTok Ltd.**”); (iii) TikTok Inc., a California corporation (“**TikTok Inc.**,” and together with ByteDance, TikTok Ltd., and, upon its joinder to this Agreement, TikTok U.S. Data Security Inc. (“**TTUSDS**”), the “**Transaction Parties**”); and (iv) [•], (together, the “**CFIUS Monitoring Agencies**,” or “**CMAs**,” and the CMAs together with the Transaction Parties, the “**Parties**”) on behalf of the Committee on Foreign Investment in the United States (“**CFIUS**”).

**RECITALS**

WHEREAS, CFIUS received written notification, dated May 27, 2020, including all information and documentary materials subsequently submitted in connection therewith, pursuant to Section 721 of the Defense Production Act of 1950, as amended (“**Section 721**”), of a transaction that was the subject of CFIUS Case 20-100;

WHEREAS, the transaction involved the merger of a wholly owned subsidiary of ByteDance with and into musical.ly (“**Musical.ly**”), a Cayman Islands exempted company, on November 23, 2017 (the “**Transaction**”);

WHEREAS, CFIUS determined that the Transaction constituted a “covered transaction” for purposes of Section 721;

WHEREAS, CFIUS undertook a review and investigation of the effects of the Transaction on the national security interests of the United States, including a risk-based analysis, as required by Section 721, and determined that there were risks to the national security of the United States that arose as a result of the Transaction;

WHEREAS, CFIUS informed ByteDance, by a letter dated July 30, 2020, that CFIUS had not identified any mitigation options that would resolve CFIUS’s concerns regarding the national security risks arising from the Transaction;

WHEREAS, pursuant to Section 721, CFIUS referred the Transaction to the President of the United States;

WHEREAS, the President of the United States determined that provisions of law, other than Section 721 and the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), do not provide adequate and appropriate authority to protect the national security of the United States;

WHEREAS, the President of the United States issued the Order of August 14, 2020, Regarding the Acquisition of Musical.ly by ByteDance Ltd. (85 Fed. Reg. 51,297 (Aug. 19, 2020)) (“**August 14 Order**”) prohibiting the acquisition by ByteDance of Musical.ly to the extent that Musical.ly or any of its assets is used in furtherance or support of, or relating to, Musical.ly’s

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

activities in interstate commerce in the United States (“**Musical.ly in the United States**”), prohibiting ByteDance’s direct or indirect ownership of any interest in Musical.ly in the United States, and in order to effectuate the August 14 Order, on such written conditions as CFIUS may impose, requiring ByteDance, its subsidiaries, affiliates, and Chinese shareholders to divest all interests and rights in: (i) any tangible or intangible assets or property, wherever located, used to enable or support ByteDance’s operation of the TikTok application in the United States, as determined by CFIUS; and (ii) any data obtained or derived from TikTok application or Musical.ly application users in the United States (clauses (i) and (ii), collectively, the “**Divestment**”);

WHEREAS, the August 14 Order authorizes CFIUS, until such time as the Divestment is completed and verified to the satisfaction of CFIUS, to implement measures it deems necessary and appropriate to verify compliance with the August 14 Order and to ensure that the operations of the TikTok application are carried out in such a manner as to ensure protection of the national security interests of the United States;

WHEREAS, ByteDance filed a petition for review of the August 14 Order and the related CFIUS actions in the U.S. Court of Appeals for the District of Columbia Circuit on November 10, 2020 (the “**Petition**”), and the adjudication of such action has been held in abeyance pending ongoing discussions with CFIUS;

WHEREAS, without admission of fault or liability, ByteDance and the CMAs, on behalf of CFIUS, are entering into this Agreement with the understanding that this Agreement will resolve the findings and concerns reflected in the August 14 Order, including the aforementioned Petition; and

WHEREAS, each of the Transaction Parties as of the Effective Date affirms that it is acknowledging and entering into this Agreement with the understanding that: (i) there is no presumption that a waiver or exception will be granted to any provision of this Agreement; and (ii) failure to abide by this Agreement is subject to all remedies available to the U.S. Government (“**USG**”), including those stated herein;

NOW, THEREFORE, pursuant to applicable law, including Section 721 and the August 14 Order, the CMAs, acting on behalf of CFIUS, hereby enter into this Agreement with the Transaction Parties:

**ARTICLE I**

**DEFINITION OF TERMS**

**Definitions.** As used in this Agreement, capitalized terms shall be defined as set forth below; *provided* that capitalized terms used in this Agreement and not defined in this Article I shall have the meanings assigned to them elsewhere in the Agreement:

1.1 “**Access**” means to, or the right or ability to: (1) enter a physical space (“**Physical Access**”); or (2) obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

view the subject data or systems in any form, directly or indirectly, whether remotely or electronically, including through information technology (“IT”) systems, cloud computing platforms, networks, security systems, software, and hardware (“**Logical Access**”). Access shall be construed broadly to include rather than exclude considered conduct.

1.2 “**Affiliate**” or “**Affiliates**” means, with respect to a specified Person, another Person that directly or indirectly, through one or more intermediaries, Controls, is Controlled by, or is under common Control with the Person specified; *provided* that for purposes of this Agreement, (i) TTUSDS and its Personnel shall not be considered Affiliates of ByteDance, and (ii) third-party shareholders of ByteDance also shall not be considered Affiliates of ByteDance.

1.3 “**Architecture Diagrams**” means one or more high-level outlines, using functional blocks and line illustrations for graphical description, of the end-to-end system concept and relationships, constraints, and boundaries between components for or supporting the TikTok U.S. App or TikTok U.S. Platform and that include detailed explanations or annotations identifying: (1) operational functionality; (2) ownership, control, and Logical Access rights, capabilities, and limitations; and (3) system input and output capabilities and limitations.

1.4 “**CFIUS Restricted Persons**” means, wherever located: (1) the government of any country identified in 22 C.F.R. §§ 126.1(d)(1) and (2) (each, a “**CFIUS Restricted Country**”) or any department, agency, or instrumentality thereof; (2) any Person organized, domiciled, headquartered, or with its principal place of business in a CFIUS Restricted Country; (3) any natural Person with nationality of a CFIUS Restricted Country who is not also (a) a U.S. citizen, (b) lawfully admitted for permanent residence as defined by 8 U.S.C. § 1101(a)(20), or (c) a protected individual as defined by 8 U.S.C. § 1324b(a)(3); or (4) any natural Person working or residing in a CFIUS Restricted Country. CFIUS Restricted Persons include any Person who, to the best of the Transaction Parties’ knowledge based on information reasonably available to them, is owned, Controlled by, or acting on behalf of a CFIUS Restricted Person; *provided, however*, that for purposes of this Agreement, TTUSDS shall not be considered a CFIUS Restricted Person.

1.5 “**Content Delivery Network**” or “**CDN**” means servers and related infrastructure that is used for the delivery of static and live content to the TikTok U.S. App (including livestreaming and communication services) that require geographical distribution to address latency issues and cannot reside exclusively within the TTP’s secure cloud infrastructure.

1.6 “**Content Promotion and Filtering**” means the promotion or filtering of content on the TikTok U.S. App outside the context of the Recommendation Engine, either through human intervention or technical measures, including relevant algorithms, rules, logic and guidelines.

1.7 “**Control**” (including the terms “**Controlled by**” and “**under common Control with**”) means the power, direct or indirect, whether or not exercised, to determine, direct, or decide important matters affecting a Person, whether by ownership of equity interests, contract, or otherwise.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

1.8 “**Creator**” means a TikTok U.S. User who has a contractual relationship with TikTok Inc. or one of its Affiliates (other than contractual relationships applicable to all TikTok U.S. Users, e.g., acceptance of the Terms of Service) for the purpose of promoting the individual or his or her brand, to earn revenue from his or her creative output, or for another promotional purpose that is intended to advance the commercial interests, following, or brand of the individual.

1.9 “**Data Flow Diagrams**” means one or more high-level outlines, using functional blocks and line illustrations for graphical description and detailed explanation, of the end-to-end flow of data to support or operate the TikTok U.S. App or TikTok U.S. Platform, including what data or information will be input and output from the system, where the data or information will come from and go to, and where the data or information will be stored. Data Flow Diagrams shall also identify: (1) the operation performed; and (2) ownership, control, and Logical Access rights, capabilities, and limitations.

1.10 “**Dedicated Transparency Center**” or “**DTC**” means physical facilities, processing resources, and network storage that are established by ByteDance in the DTC Approved Countries for the express purpose of enabling security inspections, reviews, and verification of the Source Code and Related Files by TTUSDS, the TTP, and other third parties pursuant to this Agreement.

1.11 “**Excepted Data**” means each of the following:

(1) data that Creators affirmatively authorize to be shared, or otherwise initiate the sharing, with TikTok Inc. or its Affiliates for the purpose of advancing the Creators’ commercial position on the TikTok U.S. App;

(2) data fields in the formats specified in Annexes A and B hereto that are: (i) categories of engineering and business data metrics or (ii) categories of interoperability data, respectively;

(3) data fields in the formats specified in Annex C that are categories of e-commerce data for transactions conducted through the TikTok U.S. App and TikTok U.S. Platform (“**E-Commerce Data**”), *provided* that:

(i) the data is necessary for commercial purposes related to the sale of the goods and services initiated by the TikTok U.S. User, including the data required to be shared with third parties involved in the transaction;

(ii) prior to the use of said data as E-Commerce Data, a TikTok U.S. User is notified that such data may be shared outside the United States with ByteDance and affiliates for the purposes described in the aforementioned subparagraph; and

(iii) after one (1) year from the date of sale, E-Commerce Data shall be maintained exclusively by TTUSDS except when the data is required to fulfill an

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

authorized e-commerce function as described in Annex C, which may be modified in consultation with the Security Committee through a protocol approved by the CMAs;

(4) hashes of username, phone number, email address, or OpenID, solely for the purpose of determining whether a user should be routed to the TikTok U.S. Platform, shall not be considered Protected Data; and

(5) additional categories of data, as approved by the CMAs, in their sole discretion pursuant to Section 11.1

1.12 **“Executable Code”** means the binary, machine-readable Software code derived from Source Code and Related Files.

1.13 **“Existing Network Diagram”** means a diagram providing a complete description of the Transaction Parties' network topology, router and server technology of its U.S. network and any U.S. networks of its Affiliates for operating or supporting the TikTok U.S. App or TikTok U.S. Platform as of the Effective Date.

1.14 **“Key Management”** means any Personnel involved in the leadership of TTUSDS, including the general manager, president, chief executive officer, chief information officer, chief technology officer, chief operating officer, general counsel, or equivalent positions (to the extent that such positions exist), such other officers who directly report to the TTUSDS Board or the TTUSDS general manager or equivalent, security leadership roles, and any Personnel of TTUSDS designated as Key Management by the CMAs in their sole discretion pursuant to Section 5.1.

1.15 **“Lawful U.S. Process”** means U.S. federal, state, or local orders or authorizations, and other orders or legal process, statutory authorizations, or certifications from U.S. federal, state, or local law enforcement officials for Access to or disclosure of information, user communications, or content.

1.16 **“Malicious Code”** means code that facilitates the circumvention of this Agreement, facilitates surveillance by unauthorized parties, or delivers nefarious applications or programs to the devices of TikTok U.S. Users; and/or software or firmware intended to perform an unauthorized process that will have adverse impacts on the confidentiality, integrity, or availability of a system including a virus, worm, trojan horse, spyware, forms of adware, or any other code-based entity that infects a host.

1.17 **“Master Services Agreement”** or **“MSA”** means the master services agreement among ByteDance, TTUSDS, and the TTP (the first TTP being Oracle Corporation (**“Oracle”**)).

1.18 **“NIST”** means the National Institute of Standards and Technology.

1.19 **“Person”** means any individual or entity.

1.20 **“Personal Identifier Information”** means an individual's: (1) full name (last, first, middle name); (2) all other names and aliases used; (3) business address; (4) country and

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

city of residence; (5) date of birth; (6) place of birth; (7) U.S. Social Security number (where applicable); (8) national identity number, including nationality, date and place of issuance, and expiration date (where applicable); (9) U.S. or foreign passport number (if more than one, all must be fully disclosed), nationality, date and place of issuance, and expiration date and, if a U.S. visa holder, the visa type and number, date and place of issuance, and expiration date; and (10) dates and nature of foreign government and foreign military service (where applicable), other than military service at a rank below the top two non-commissioned ranks of the relevant foreign country.

1.21 **“Personnel”** means any employee, director, officer, manager, agent, contractor, or other representative of an entity, and includes the respective successor or assigns of the foregoing.

1.22 **“Protected Data”** means any data collected from a TikTok U.S. User, including: (1) user data (including username, password, email address, phone number, nickname, birth date or age, profile thumbnail, biographical information, genetic or biometric data or information, appearance, device contacts list, and any third-party social media credentials, list of third-party applications installed on the same device as the TikTok U.S. App, or payment account information); (2) user content (including videos, music, pictures, articles, hashtags, captions, comments, direct messages, and other material uploaded by users including private or unpublished content); (3) behavioral data (including user interaction with content, such as likes given, likes received, not interested, video playtime, shares, follows, followers, block list, favorites, downloads, log-in history, browsing history, search history, keystroke patterns and rhythms, and purchase history); (4) any data that is collected on U.S. user interaction with content on the TikTok U.S. Platform as an input into the Recommendation Engine, including video completion, not interested markings, and video viewing time, (**“User Interaction Data”**); (5) device and network data (including Internet Protocol (**“IP”**) address, cookie data, device identifiers, MAC address, mobile carrier, network settings, time zone settings, app and file names, device clipboard, device contacts, device calendars, device media, source of user, Android ID, Apple ID for Advertisers, Google Advertising ID, any other ID for Advertisers, device model and characteristics, operating system (**“OS”**), list of installed apps, system language and region, and geographic location, such as the city, state, country, or GPS coordinates of the device’s location); (6) any other personally identifiable information; and (7) any other information provided by or derivative of TikTok U.S. Users in connection with their use of the TikTok U.S. App. Protected Data includes all of the foregoing even if de-identified, anonymized, or aggregated but shall not include Excepted Data or Public Data. TikTok U.S. Platform systems log data that has had all Protected Data removed by the TTP shall not be Protected Data.

1.23 **“Public Data”** means data that is generally accessible to users of the TikTok U.S. App, including videos, comments, and similar user content and includes each of the following:

- (1) feature categories as specified in Annex E;
- (2) any content that TikTok U.S. Users affirmatively decide to make public;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(3) any hash of Public Data; and.

(4) additional feature categories added pursuant to Section 11.2.

1.24 **“Recommendation Engine”** means the algorithms and related data models used by the TikTok U.S. App and TikTok U.S. Platform to rank content and select content for recommendation to TikTok U.S. Users, including their Source Code and Related Files, such as machine learning processes, statistical weights and parameters, and outputs. For the avoidance of doubt, the Recommendation Engine does not include the Content Promotion and Filtering algorithms.

1.25 **“Resident Sole U.S. Citizen”** means an individual who holds U.S. citizenship and currently has, and maintains for the duration of his or her responsibilities in connection with this Agreement, residency in the United States as determined by meeting the substantial presence test set forth in 26 U.S.C. § 7701(b)(3), and who is not a citizen of any other country.

1.26 **“Resident U.S. Citizen”** means an individual who holds U.S. citizenship and currently has, and maintains for the duration of his or her responsibilities in connection with this Agreement, residency in the United States as determined by meeting the substantial presence test set forth in 26 U.S.C. § 7701(b)(3).

1.27 **“Software”** means a set of instructions that are generated from source code and used to operate electronic devices and execute specific tasks on a device or a system, including executable code, tools, platforms, and related user manuals.

1.28 **“Source Code and Related Files”** means: (1) all of the actual, human-intelligible Software code, including files, libraries, data schemas and algorithms from ByteDance and its Affiliates used to operate the TikTok U.S. App or TikTok U.S. Platform; and (2) any other documentation, specifications, and artifacts from ByteDance and its Affiliates that are used to design, develop, maintain, modify, operate, improve, or define the behavior of the TikTok U.S. Platform or the TikTok U.S. App. For the avoidance of doubt, “Source Code and Related Files” shall not include (1) or (2) when developed by TTUSDS.

1.29 **“Source Code Review Diagrams”** means one or more high-level outlines, using descriptive functional blocks and line illustrations for graphical description, of the process for reviewing Source Code and Related Files that identify: (1) the operation performed; (2) who among the Transaction Parties or the TTP has obligations or actions to perform; and (3) who among the Transaction Parties or TTP has ownership, Logical Access, or control.

1.30 **“SPAC Transaction”** means the consummation of a transaction or series of transactions (whether by merger, consolidation, or transfer or issuance of equity interests or otherwise) whereby a special purpose acquisition company acquires all of the equity interests of a company (or any surviving or resulting company) or a transaction having a similar effect.

1.31 **“Test Accounts”** means accounts established by the Transaction Parties and verified and approved by the TTP as accounts not associated with any individual for the purpose

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

of testing operational functionality and enabling continued innovation and refinement of user features of the TikTok U.S. App and TikTok U.S. Platform.

1.32 **“TikTok Global App”** means each of the following, in their current and future versions and as the service may evolve:

(1) the TikTok-branded application(s), including any regional or other jurisdiction-specific versions, that are accessible by the public through an online application store (e.g., one offered by Apple, Google, or Amazon) or an equivalent method of accessing the application and that allows users to consume, create, share, and otherwise interact with content; and

(2) the TikTok web application(s) that are used to provide web browser users with a TikTok product experience similar to the product experience provided through the TikTok-branded application(s) described in clause (1) of this definition on mobile devices.

1.33 **“TikTok U.S. Application”** or **“TikTok U.S. App”** means all versions of the TikTok Global App provided to, or accessible by, TikTok U.S. Users.

1.34 **“TikTok U.S. Platform”** means the infrastructure, including the IT systems, cloud computing platforms, servers, networks, security systems, and equipment (software and hardware), and all related services and program elements that host, operate, maintain, deploy, support, and run the service and storage facilities for the TikTok U.S. App. For avoidance of doubt, the Recommendation Engine shall be contained and deployed from within the TikTok U.S. Platform.

1.35 **“TikTok U.S. User”** means:

(1) an individual signing into the TikTok Global App through an account that, at the time of registration, was attributable to the United States based upon any of the following means (with respect to Sections 1.32(1)(i)–(iv), in order of priority):

(i) Country code of the device subscriber identity module (“**SIM**”) card;

(ii) IP Address;

(iii) Mobile Country Code associated with the mobile subscription of the device; or

(iv) OS/System Region (i.e., obtained via an application programming interface (“**API**”) call provided by the OS (either Android or iOS), which returns a country code);

(2) an individual signing into the TikTok Global App through an account that has been designated a “TikTok U.S. User” account pursuant to Section 11.3; or



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(3) for users who are not signing into the TikTok Global App with a registered account, a device that first accesses the TikTok Global App from an IP address located in the United States.

(4) For the avoidance of doubt, Test Accounts shall not be considered TikTok U.S. Users.

1.36 **“Trust and Safety Moderation”** means the removal or downgrading of content or user accounts that are viewable or eligible for recommendation on the TikTok U.S. App, either through technical measures or human review, in order to meet trust and safety guidelines. Trust and Safety Moderation excludes Content Promotion and Filtering.

1.37 **“Trusted Technology Provider” or “TTP”** means Oracle in its capacity as the TTP, or any successor TTP, in each case operating under an MSA consistent with the requirements of Section 8.2.

1.38 **“United States” or “U.S.”** means the several States, the District of Columbia, and any territory or possession of the United States.

**ARTICLE II**

**FORMATION OF TIKTOK U.S. DATA SECURITY INC.**

2.1 **Formation of TikTok U.S. Data Security Inc.** By no later than one-hundred and eighty (180) days following the Effective Date (the **“Operational Date”**), ByteDance shall establish TTUSDS as a wholly owned subsidiary of TikTok Inc. that is incorporated in the United States. The Transaction Parties may request an extension of the Operational Date no later than one-hundred and sixty-six (166) days following the Effective Date, in which case the Transaction Parties shall submit to the CMAs a written request that includes a summary of the actions taken to date, the reason for the delay, and the requested new Operational Date. The CMAs may non-object, non-object with predicate conditions, or object to the request for an extension in their sole discretion. In the event that the CMAs non-object with predicate conditions to the request, the Operational Date shall be extended only if the Transaction Parties meet the specified conditions to the satisfaction of the CMAs in the CMAs' sole discretion. In the event that the CMAs object to the request, the Operational Date shall not be extended. If the CMAs do not either object or non-object with predicate conditions to the request within seven (7) days of receipt, the lack of action shall constitute a non-objection.

2.2 **Headquarters.** By no later than the Operational Date and at all times thereafter, ByteDance shall ensure that TikTok Inc. and TTUSDS maintain their respective headquarters offices exclusively in the United States and that TTUSDS's offices are not co-located with any offices of ByteDance or its Affiliates without prior written approval of the CMAs. Immediately following the Operational Date, TTUSDS shall also ensure that its headquarters offices are maintained in the United States and that its offices are not co-located with any offices of ByteDance or its Affiliates without prior written approval of the CMAs. Following the

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Operational Date, TTUSDS shall ensure that only its Personnel are responsible for the day-to-day operations and management of TTUSDS's business.

2.3 TTUSDS Joinder. By no later than the Operational Date, ByteDance shall ensure that TTUSDS joins this Agreement by submitting to the CMAs a joinder agreement signed by a duly authorized representative of TTUSDS that is in the form at Annex D.

2.4 CFIUS Functions. By no later than the Operational Date and at all times thereafter, the Transaction Parties shall ensure that TTUSDS owns or has a license to, and manages, all of the assets and employs all of the Personnel related to the following aspects of the TikTok U.S. App's operations (collectively, the "**CFIUS Functions**"):

(1) overseeing the storage and protection of Protected Data, including through TTUSDS's activities pursuant to the MSA;

(2) facilitating and assisting with the TTP's receipt and inspection of Source Code and Related Files via the DTC, as well as TTUSDS's and the TTP's deployment of Executable Code;

(3) TikTok U.S. App trust and safety operations and functions that require Access to any Protected Data (except as otherwise expressly provided for in this Agreement);

(4) content, user, and advertising operations, including Content Promotion and Filtering, that require Access to any Protected Data;

(5) identifying and implementing remediations for the Recommendation Engine in response to the review by the TTP pursuant to this Agreement;

(6) overseeing, authorizing, and documenting the sale or transfer of Protected Data to any third parties, to the extent that such sale or transfer is permitted under this Agreement; and

(7) maintaining primary responsibility for ensuring day-to-day compliance with this Agreement.

2.5 Enabling TTUSDS. By no later than the Operational Date, and to ensure that TTUSDS can effectively and independently perform the CFIUS Functions, ByteDance shall, and shall ensure that its Affiliates:

(1) take all necessary actions to ensure that all commercial agreements with third parties for the operation and delivery of the TikTok U.S. App and TikTok U.S. Platform are transferred, assigned, licensed, or otherwise contributed, as applicable, to TTUSDS;

(2) subject to Section 5.4, transfer the employment agreements of all Personnel responsible for performing the CFIUS Functions to TTUSDS;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(3) enter into a license and service agreement with TTUSDS, to be developed in coordination with the CMAs and the TTP to ensure that the terms of such license and service agreement are consistent with this Agreement, that:

(i) ensures TTUSDS has all necessary rights to ByteDance technology, including Source Code and Related Files and all updates thereto, Executable Code, and other Software required to operate and manage the TikTok U.S. App and TikTok U.S. Platform, for the purposes set forth in this Agreement;

(ii) provides TTUSDS with support to perform the CFIUS Functions;  
and

(iii) provides that in the event of a conflict between the terms of such license and service agreement and this Agreement, the terms of this Agreement shall prevail; and

(4) sub-license to TTUSDS, or arrange for new licenses for TTUSDS to, all third-party Software and technologies for which ByteDance is a licensee that are necessary to operate and manage the TikTok U.S. App and TikTok U.S. Platform.

2.6 Formation and Operational Plan. ByteDance shall submit a plan to the CMAs within fourteen (14) days following the Effective Date that describes the steps ByteDance will take to:

(1) ensure that TTUSDS owns or has a license to, and manages, all of the assets and employs all Personnel related to the CFIUS Functions;

(2) contribute, assign, or license to TTUSDS, as applicable, all assets necessary to comply with this Agreement; and

(3) ensure that TTUSDS will become operational by the Operational Date, which at a minimum means that TTUSDS can manage its day-to-day operations and perform the CFIUS Functions as set forth in this Agreement separate and apart from ByteDance and its Affiliates.

2.7 TTUSDS Independence. By no later than the Operational Date and at all times thereafter, ByteDance shall not play any role in or make any attempt to influence, determine, direct, or decide the operations, management, or leadership of TTUSDS, except as otherwise expressly provided for in this Agreement. ByteDance shall ensure that none of its Affiliates plays any role in or makes any attempt to influence, determine, direct, or decide the operations, management, or leadership of TTUSDS, except as otherwise expressly provided for in this Agreement.

2.8 TTUSDS Funding. ByteDance shall provide sufficient financial resources to enable TTUSDS to fully perform the CFIUS Functions and fulfill its obligations under this Agreement. TTUSDS shall promptly notify the Third-Party Monitor and CMAs if TTUSDS

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

believes, in its sole discretion, that it lacks sufficient funds to perform the CFIUS Functions and fulfill its obligations under this Agreement. The Transaction Parties shall provide semi-annual updates to the Third-Party Monitor and CMAs regarding the budgeting and funding of TTUSDS.

2.9 Ownership of TTUSDS. At least seven (7) days prior to entering into any agreement or completing any transaction through which: (1) any Person other than TikTok Inc. will acquire a direct economic or voting interest in TTUSDS; or (2) there will be a greater than five percent (5%) change to the ownership of the indirect economic or voting interests in ByteDance, TikTok Inc., or TTUSDS as of the Effective Date, the Transaction Parties shall provide written notification to the CMAs of the identity of the Person to own the interest, the percentage and nature of the interest to be owned, and all relevant transaction documents and side agreements; *provided, however*, that prior notice of any transaction described in Section 2.9(2) shall not be required if such transaction would not involve a change in the direct economic or voting interests in TikTok Inc., TTUSDS, or any other subsidiary of ByteDance, and ByteDance is a publicly listed company at the time of such transaction. The Transaction Parties shall also submit to the CMAs a quarterly summary capitalization table of ByteDance identifying all shareholders holding a more than one percent (1%) equity interest or voting interest in ByteDance as of the end of the quarter.

### **ARTICLE III**

#### **GOVERNANCE OF TIKTOK U.S. DATA SECURITY INC.**

3.1 TTUSDS Board Composition. The Transaction Parties shall ensure that TTUSDS is at all times governed by a board of directors (the “**TTUSDS Board**”) of three (3) directors who: are Resident Sole U.S. Citizens, unless otherwise approved by the CMAs; have no current or prior employment, or contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates; have strong credentials in national security or extensive experience in IT, cybersecurity, or data security; and have, or are eligible for, a U.S. personnel security clearance (the “**Security Directors**”).

(1) The Transaction Parties shall ensure that the composition of the TTUSDS Board is limited exclusively to the Security Directors. The Transaction Parties shall designate, subject to CMA non-objection concurrent with the appointment process in Section 3.2, one of the Security Directors as Chair of the TTUSDS Board (the “**TTUSDS Chair**”), and a second Security Director as Chair of the Security Committee established pursuant to Section 3.8. For the avoidance of doubt, the Transaction Parties may appoint the TTUSDS Chair as chair of the Security Committee. Subject to CMA approval, the Transaction Parties shall be able to set term limits and/or stagger the terms for each Security Director, the expiration of a Security Director term being treated as a vacancy pursuant to Section 3.09 of the Agreement, including for purposes of triggering the timing requirements for replacements.

3.2 Initial TTUSDS Board Appointments. The Transaction Parties shall ensure that no Security Director is appointed or otherwise becomes a director without the prior non-objection of the CMAs. At least [X] days prior to the Operational Date, the Transaction Parties shall submit to the CMAs complete Personal Identifier Information, a *curriculum vitae* or similar

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

professional synopsis, contact information, and any other information requested for each Security Director nominee for the CMAs to assess whether the nominee can effectively perform the functions set forth in this Agreement. The Transaction Parties shall ensure that the CMAs may, at their request, interview the Security Director nominees. If the CMAs do not object in writing within twenty-one (21) days following receipt of all necessary information about the Security Director nominees, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to one or more Security Director nominees, the Transaction Parties shall nominate a different candidate within twenty-one (21) days following receipt of any such objection, subject to the same procedures as the initial nomination. The Transaction Parties shall ensure that a Security Director is appointed for each Security Director position on the TTUSDS Board following the non-objection of the CMAs by no later than the Operational Date. After the Operational Date, if all the board seats are not filled, the Transaction Parties shall ensure that any initial Security Director nominee is appointed within three (3) days following the non-objection of the CMAs. For the avoidance of doubt, the appointment of replacement nominees shall be subject to the terms of Section 3.09 below.

3.3 TTUSDS Voting. The Transaction Parties shall ensure that each Security Director is entitled to cast one (1) vote on each matter presented to the TTUSDS Board and any committee thereof, and that all decisions of the TTUSDS Board and any committee thereof require the affirmative vote of: a majority of the directors in office.

3.4 TTUSDS Quorum. TTUSDS shall ensure that a minimum of two (2) Security Directors, which must include the chair of the Security Committee, are required to be present in order to establish a quorum at any meeting of, or for any action by, the TTUSDS Board or any committee thereof. TTUSDS shall ensure that neither the TTUSDS Board nor any committee thereof convenes or takes any action in the absence of a quorum. TTUSDS shall further ensure that, in the event that the chair of the Security Committee is vacant or otherwise unable to fulfill his or her role, or fails to attend a meeting twice without justification, the Security Directors present and voting select one of the other Security Directors to serve as acting chair of the Security Committee for the purposes of establishing quorum and breaking ties.

3.5 TTUSDS Board Attendance and Meetings. TTUSDS shall ensure that attendance at all meetings of the TTUSDS Board and any committee thereof is limited to the Security Directors, the TTUSDS general manager or equivalent, the TTUSDS General Counsel, the Corporate Secretary of the TTUSDS Board, the Security Officer, the Third-Party Monitor, and such other individuals whose attendance is approved in advance by the CMAs, and, with respect to meetings of the Security Committee, the Technology Officer.

(1) TTUSDS shall ensure that apart from those individuals expressly permitted to attend meetings of the TTUSDS Board under this Section 3.5, any other observers or attendees at meetings of the TTUSDS Board or any committee thereof are approved in writing in advance by the CMAs. At least seven (7) days in advance of a meeting of the TTUSDS Board or any committee thereof, TTUSDS shall submit a written request to the CMAs of any individual, other than those specifically listed in this Section 3.5, who is proposed to attend the meeting and provide their title, affiliation, and the purpose of their participation.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(2) TTUSDS shall ensure that the Security Officer and Third-Party Monitor are given advance notice of, and the opportunity to, participate in all meetings of the TTUSDS Board and any committee thereof in a non-voting observer capacity, and that the Technology Officer participates in all meetings of the Security Committee in a non-voting observer capacity.

(3) TTUSDS, in conjunction with the Security Committee, shall submit to the Security Officer, Third-Party Monitor, and CMAs: (1) copies of all board and committee materials at least one (1) day prior to any meeting, unless the Security Committee certifies in writing that exceptional circumstances require an emergency meeting of the TTUSDS Board, and in such case TTUSDS shall submit concurrent notice to the Security Officer, Third-Party Monitor, and CMAs; and (2) copies of the complete unredacted meeting minutes no more than seven (7) days following any board or committee meeting.

3.6 Security Director Duties. The Transaction Parties shall ensure that in exercising their duties, the Security Directors owe fiduciary duties exclusively to the CMAs and TTUSDS; *provided* that the Security Directors shall discharge their duties in a manner that they reasonably believe in good faith to be, in descending order: first, in the national security interest of the United States as determined by the CMAs; and second, where not inconsistent with the national security interest of the United States, in the best interests of TTUSDS, in each case subject to this Agreement. Following their appointment as Security Directors and for so long as they serve on the TTUSDS Board, TTUSDS shall ensure that none of the Security Directors has any employment, contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates. The terms of compensation for the Security Directors, including any benefits or stock incentive awards of any of the Transaction Parties, shall be negotiated between TikTok Inc. and the Security Director and shall be paid by TTUSDS. The terms of compensation, to include the grant of any stock incentive awards, shall be fixed for the Security Directors' terms.

3.7 Security Committee. By no later than the Operational Date, the Transaction Parties shall ensure that the TTUSDS Board forms a permanent, board-level committee composed exclusively of the Security Directors to serve as the committee with the full and sole authority to decide all matters related to data security, cybersecurity, and national security for TTUSDS (the "**Security Committee**"). The Transaction Parties shall ensure that the TTUSDS governance documents reflect the Security Committee's responsibilities and provide that such governance documents cannot be further amended to eliminate the Security Committee or modify the Security Committee's rights and responsibilities without the prior written consent of the CMAs. TTUSDS shall ensure that the presence of at least two (2) Security Directors, including the Security Director who is chair of the Security Committee, is required to establish quorum for the Security Committee and that all meetings of, and action by, the Security Committee include the Security Officer. TTUSDS shall ensure that the Security Committee:

(1) serves as the primary liaison between the TTUSDS Board and the CMAs, provides timely responses to inquiries from the CMAs, and maintains availability, upon reasonable notice from the CMAs, for discussions with the CMAs, in each case on matters relating to TTUSDS' governance and compliance with this Agreement;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(2) oversees the implementation of all policies, procedures, protocols, and other matters relating to the TTUSDS' compliance with this Agreement;

(3) oversees and periodically reviews TTUSDS' activities in performance of the CFIUS Functions;

(4) meets regularly, and at least quarterly, to perform its obligations under this Agreement; and

(5) annually certifies TTUSDS's compliance with this Agreement to the CMAs within seven (7) days of each anniversary of the Effective Date. Such certification shall be signed by all members of the Security Committee and may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall be deemed to constitute one and the same certification.

**3.8 TTUSDS Recordkeeping and Related Certifications.**

(1) TTUSDS shall ensure that the TTUSDS Board prepares and retains all preparatory materials, records, journals, and minutes of all meetings and deliberations of the TTUSDS Board and any committee thereof for inspection by the CMAs for a period of at least five (5) years.

(2) TTUSDS shall provide to the CMAs, within seven (7) days following a meeting of the TTUSDS Board or any committee thereof:

(i) all materials provided or used at the meeting, including board presentations and related exhibits, and final versions of any draft materials previously provided;

(ii) copies of meeting minutes certified by a Security Director to be accurate and complete as to the topics discussed at each meeting of the TTUSDS Board and any committee thereof;

(iii) a roster of attendees at the meeting; and

(iv) a signed certification by a Security Director in attendance that the meeting was conducted in accordance with the obligations set forth in this Agreement.

**3.9 TTUSDS Director Vacancies.** TTUSDS shall notify the Security Committee, Security Officer, Third-Party Monitor, and CMAs within two (2) days of receiving notice of any Security Director's planned or actual resignation, death, disability, or other circumstance creating a vacancy on the TTUSDS Board. Within twenty-one (21) days following a vacancy, TikTok Inc. shall nominate an individual to fill such vacancy consistent with the initial appointment process under Section 3.2.

**3.10 TTUSDS Director Removal.** The Transaction Parties shall ensure that any removal or replacement of a Security Director is subject to the following processes:

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(1) The Transaction Parties shall have the right to remove any Security Directors subject to all conditions included herein. The Transaction Parties shall not remove any Security Director until all of the following conditions are met: (1) TTUSDS has notified the Security Director, the Security Committee, the Security Officer, the Third-Party Monitor, and the CMAs at least twenty (20) days prior to the proposed removal date; (2) TTUSDS has provided a written justification to the CMAs for the removal with the notice provided at least twenty (20) days prior to the proposed removal date; (3) the CMAs have provided a written non-objection to the removal; and (4) a replacement has been nominated consistent with the initial appointment process under Section 3.2.

(2) The Transaction Parties shall ensure that, should the CMAs provide written notice setting forth their determination (including a written justification for the removal), in their sole discretion, that any director of the TTUSDS Board has, intentionally or through gross negligence, failed to meet his or her obligations or has undermined the effectiveness of this Agreement, the CMAs may direct the Transaction Parties to remove the director and the Transaction Parties shall promptly, and in any event within two (2) days, remove such director. Within twenty-one (21) days following such removal, TikTok Inc. shall nominate a replacement consistent with the initial appointment process in Section 3.2. The Transaction Parties may, in response to such direction, seek consultations with the CMAs to resolve the concerns associated with any director, which the CMAs may engage in at their discretion but any such consultation shall not toll the deadline to remove such director or nominate a replacement.

(3) Regardless of whether there is a vacancy among the Security Director positions, the Transaction Parties may, at their discretion, provide the names of up to five (5) nominees to serve as Security Directors for consideration by the CMAs. The CMAs may notify the Transaction Parties of their provisional approval or disapproval of the nominees to be eligible to serve as Security Directors should a position become vacant. If the CMAs provide provisional approval, TikTok Inc. shall still be required to formally nominate the potential Security Director pursuant to the initial appointment process in Section 3.2.

3.11 TTUSDS Governance Documents. ByteDance shall submit draft copies of all governance documents of TTUSDS (e.g., articles of association, bylaws, charter, and any other documents that govern TTUSDS, collectively the “**TTUSDS Governance Documents**”) to the CMAs at least fourteen (14) days prior to the Operational Date and from time to time after the Operational Date at the request of the CMAs or prior to any proposed amendment thereto. The Transaction Parties shall promptly, and in any event within five (5) days following receipt of a request from the CMAs, make any change to such governance documents requested by the CMAs to incorporate the terms of this Agreement, to the CMAs’ satisfaction in their sole discretion.

(1) ByteDance shall ensure that the TTUSDS Governance Documents cover all matters within the authority of TTUSDS shareholder and the TTUSDS Board. The Transaction Parties shall ensure that the consent of the TTUSDS shareholder is not required for any decision by the TTUSDS Board or any committee thereof, however, the TTUSDS Board shall not have the authority to approve the following material corporate actions without the affirmative consent of the TTUSDS shareholder:



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(i) Corporate and tax structuring and intercompany matters, including requesting TikTok Inc. make capital contributions, determining TTUSDS' annual net profits or net losses for financial accounting and tax purposes, or making profit distributions to TikTok Inc.;

(ii) Entering into, amending, modifying, renewing, terminating, or waiving any rights under any material agreement or arrangement with the TTP related to the service levels, fees, liability allocations, indemnifications, or such other matters;

(iii) Corporate policies implemented at TTUSDS establishing the term, compensation and benefits parameters for Key Management Personnel, including the general manager, head of human resources, head of technology, and head of finance, or their equivalents consistent with ByteDance's global corporate policies;

(iv) Entering into a new material line of business of TTUSDS or its subsidiaries; making any material changes to the scope of any existing lines of business, products, or services of TTUSDS or its subsidiaries; or otherwise making any material change to the purpose or scope of the business as set forth in the Governance Documents;

(v) Issuance of new equity (including convertible instruments such as options, warrants, and convertible bonds) or any rights to subscribe for any equity (including convertible instruments such as options, warrants, and convertible bonds);

(vi) Pursuing an initial public offering or a SPAC Transaction or any other financing transaction for TTUSDS or its subsidiaries;

(vii) Entering into, amending, renewing, or terminating the following transactions, agreements, or arrangements:

(1) The sale, merger, consolidation, reorganization, dissolution, liquidation, disposal, or winding up in any manner of capital assets or businesses of TTUSDS;

(2) The merger or acquisition of the assets, equity, or business of another entity, or the issuance of equity to or a joint venture with any third party;

(3) A material investment, material licensing relationship, or other material strategic relationships in or with any third party;

(4) (x) Incurring or guaranteeing indebtedness; (y) pledging, mortgaging, leasing, or encumbering the assets of TTUSDS or any of its subsidiaries; and (z) creating or authorizing the creation of any debt security or the issuance of any liens, where the aggregate total of (x)

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

through (z) is greater than five percent (5%) of the TTUSDS annual operating budget for the given year;

(5) Any transaction that:

(A) Is with a ByteDance competitor listed in Annex F or an Affiliate of a ByteDance competitor listed in Annex F;

(B) Results in any material negative deviation from the standards for the TikTok U.S. App and TikTok U.S. Platform set by ByteDance; *provided* that such standards are consistent with this Agreement in all respects as determined by the CMAs or the Security Committee as applicable; or

(C) Violates in any material respect any contracts and license agreements among the Transaction Parties and their respective subsidiaries.

(viii) Waiver of litigation rights, or agreement of settlement or admission of liability, fault, or noncompliance of TTUSDS or its subsidiaries;

(ix) Settling any litigation or other proceedings (a) for an amount exceeding [\$1 million] individually or [\$10 million] in the aggregate per calendar year; or (b) that involve the grant of an injunction or other equitable relief or otherwise impose any material restriction on the Transaction Parties' business and their respective subsidiaries;

(x) Making any material change to the accounting policies, practices, or methodologies for TTUSDS or its subsidiaries, unless otherwise required by law;

(xi) The filing or making of any petition under the U.S. federal bankruptcy laws or any similar law or statute of any state or any foreign country;

(xii) Making any changes to the existing legal rights or preferences of the shareholder interests, rights, preferences, or privileges in the ownership and governance documents of TTUSDS or any of its subsidiaries;

(xiii) To the extent not otherwise covered above, making any amendments to the ownership and governance documents of TTUSDS or any of its subsidiaries;

(xiv) The creation of any new direct or indirect subsidiary of TTUSDS or issuance or transfer of equity of any direct or indirect subsidiary of TTUSDS, in each case, other than the creation of TTUSDS itself or of a wholly owned direct or indirect subsidiary of TTUSDS;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(xv) adoption of the overall annual budget and key performance indicators (“**KPIs**”), but only if the budget or KPIs, as applicable, do not meet the following requirements:

(1) The budget and KPIs are within the parameters set by the TikTok, Inc. Board, and presented to and discussed with the TTUSDS Board and management; provided that the TTUSDS board confirms that the budget parameters provide sufficient funding for TTUSDS consistent with Section 2.8;

(2) TTUSDS has provided the TikTok, Inc. Board a reasonable opportunity to review the budget and KPIs prior to TTUSDS Board approval; and

(3) The budget’s assumptions and projections are reasonable and consistent with the performance of TTUSDS as it develops.

(xvi) Such other matters as may be added to this list with the prior written approval of the CMAs in their sole discretion.

(2) The TTUSDS Shareholder shall be entitled to all relevant and material information necessary to make an informed decisions regarding any action or decision taken in connection with Paragraph 3.13(1) except information that the Security Committee determines in their sole discretion to be information that cannot be shared consistent with this Agreement including those matters relating to data security, cybersecurity or national security (“**Confidential Matters**”).

(3) The TTUSDS Governance Documents shall also provide that:

(i) the TTUSDS Board shall consult with the TikTok Inc. Board on determining compensation and benefits of Key Management Personnel, including the general manager, head of human resources, head of technology, and head of finance, or their equivalents. For the avoidance of doubt, the TTUSDS Board shall retain the final authority to determine the compensation and benefits of Key Management Personnel; and

(ii) the TTUSDS Board shall adopt and maintain policies that are materially consistent with corresponding policies that are produced and maintained at by the TikTok, Inc. Board of Directors to ensure consistency in operations, including, by way of example, budget planning and reporting, key performance indicators, principles on finance operations, principles on compliance and governance, principles on tax, and principles on auditing, provided such policies, as adopted by the TTUSDS Board, are consistent with this Agreement.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

**ARTICLE IV**

**GOVERNANCE OF TIKTOK INC.**

4.1 TikTok Inc. Board Composition. ByteDance and TikTok Ltd. shall ensure that TikTok Inc., at least thirty (30) days prior to the Operational Date, and at all times thereafter, is governed by a board of directors (the "**TikTok Inc. Board**") of at least five (5) directors consistent with the following composition:

(1) at least two (2) directors who are not CFIUS Restricted Persons, unless otherwise approved by the CMAs, who are employed by ByteDance or its Affiliates (the "**Inside Directors**");

(2) at least two (2) directors who are Resident U.S. Citizens or citizens of other countries of the National Technology and Industrial Base, as defined by 10 U.S.C. § 2500 ("**NTIB**"), unless otherwise approved by the CMAs, who are not employed by ByteDance or its Affiliates (the "**Outside Directors**"); and

(3) the TTUSDS Chair appointed pursuant to Section 3.1.

4.2 Business of TikTok Inc. By no later than the Operational Date, ByteDance and TikTok Inc. shall each ensure that the TikTok Inc. Board is responsible for the governance of the business related to the TikTok U.S. App and TikTok U.S. Platform other than those related to the CFIUS Functions, which shall be solely owned or licensed, and managed, by TTUSDS, and except as otherwise expressly provided for in this Agreement. Other than as they relate to compliance with this Agreement, the TikTok Inc. Board shall have exclusive management authority over the following matters:

(1) Business strategy for the United States;

(2) Coordination between the TikTok business in the United States with the rest-of-world TikTok business;

(3) Product feature development for the United States;

(4) Internal tool development to be used and deployed in the TikTok U.S. Platform;

(5) TikTok U.S. User experience, including user feedback;

(6) U.S. trust and safety;

(7) Setting standards and measuring for the TikTok business in the United States the following: core business practices, policies, and metrics, including human resources policies, KPIs, employee morale and sentiment, and compensation policies;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(8) Reviewing recruitment, hiring or termination, compensation, benefits, and performance of senior officers and managers for the United States to ensure consistency with the rest of the world and company policies;

(9) Setting facilities and real estate standards for consistency with rest-of-world real estate practices;

(10) U.S. financials and other related matters, including:

(i) Revenue, operating expenses, and related metrics;

(ii) Audits and reporting;

(iii) Budgets and forecast;

(iv) Treasury, cash, and debt;

(v) Taxes;

(vi) Valuation;

(11) Legal compliance matters unrelated to this Agreement; and

(12) such other matters that are necessary to give effect to the aforementioned listed items.

4.3 TikTok Inc. Board Voting and Quorum Requirements.

(1) TikTok Inc. shall ensure that each director of the TikTok Inc. Board is entitled to cast one (1) vote on each matter presented to the TikTok Inc. Board and any committee thereof, and that all decisions of the TikTok Inc. Board and any committee thereof require the affirmative vote of a majority of the directors in office.

(2) TikTok Inc. shall ensure that the presence of the TTUSDS Chair is required in order to establish a quorum at any meeting of, or for any action by, the TikTok Inc. Board or any committee thereof, unless the TTUSDS Chair has received written notice of such meetings and twice failed to attend without reasonable justification. Prior to holding any meeting of the TikTok Inc. Board without the presence of the TTUSDS Chair, TikTok Inc. shall notify the CMAs of the TTUSDS Chair's failure to attend and provide the relevant justification (if any). Whether the TTUSDS Chair's justification for his or her failure to attend constitutes "reasonable justification" for purposes of Section 4.3(2) shall be in the sole discretion of the CMAs. If the CMAs do not object in writing within ten (10) days following receipt of the TTUSDS Chair's justification for his or her failure to attend, the lack of action shall constitute a non-objection. TikTok Inc. shall ensure that neither the TikTok Inc. Board nor any committee thereof convenes or takes any action in the absence of a quorum.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(3) TikTok Inc. shall ensure that the affirmative vote of the TTUSDS Chair is required for any decision of the TikTok Inc. Board or any committee thereof that involves any of the following with respect to TikTok Inc. or its subsidiaries, each as determined in accordance with the TTUSDS Chair's reasonable discretion and in conformance with said Director's fiduciary duties:

(i) matters dealing with the relationship with or responsibilities of the TTP, each solely as they relate to this Agreement; and

(ii) issues that directly impact the Transaction Parties' compliance with this Agreement.

4.4 **Board Conflicts.** The Transaction Parties shall ensure the business and affairs of TikTok Inc. and TTUSDS are managed, and all corporate powers are exercised by or under the direction of, the TikTok Inc. Board and TTUSDS Board, respectively. If during a meeting of the TikTok Inc. Board, the TTUSDS Chair objects to a topic of discussion, the matter shall be tabled until the Security Committee can convene to determine whether the matter appropriately falls within the scope of Section 2.4 or 4.2.

4.5 **TTUSDS Chair Duties.** ByteDance, TikTok Ltd., and TikTok Inc. shall ensure that in exercising his or her duties, the TTUSDS Chair owes fiduciary duties exclusively to the CMAs and TikTok Inc.; *provided* that the TTUSDS Chair shall discharge his or her duties in a manner that he or she reasonably believe in good faith to be, in descending order: first, in the national security interest of the United States as determined by the CMAs; and second, where not inconsistent with the national security interest of the United States, in the best interests of TikTok Inc., in each case subject to this Agreement.

4.6 **TikTok Inc. Recordkeeping.** TikTok Inc. shall ensure that the TikTok Inc. Board prepares and retains all records, journals, and minutes of all meetings and deliberations of the TikTok Inc. Board and any committee thereof for a period of at least five (5) years for inspection by the CMAs.

4.7 **TTUSDS Chair Vacancy and Removal.**

(1) The TTUSDS Chair shall be subject to the same vacancy and removal provisions as in his or her capacity as a Security Director of the TTUSDS Board in accordance with Section 3.10.

(2) The TTUSDS Chair may be removed from the TikTok Inc. Board on the same terms and conditions as set forth for Security Directors in Section 3.10. In the event of a vacancy in the TTUSDS Chair position, ByteDance shall select one (1) of the remaining Security Directors of the TTUSDS Board to assume the TTUSDS Chair position on the TikTok Inc. Board, subject to prior notice to and non-objection by the CMAs.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(3) For the avoidance of doubt, the lapse of a term limit for any TTUSDS Chair of the TikTok Inc. Board shall trigger the processes under this Section 4.7 for the replacement of such TTUSDS Chair, including the timing requirements for replacements.

4.8 TTUSDS Board and TikTok Inc. Board Coordination. Notwithstanding any other provision of this Agreement, the TTUSDS Board and TikTok Inc. Board shall be permitted to meet jointly to facilitate discussion of any matters not prohibited by this Agreement. Until the one-year anniversary of the Operational Date, the TTUSDS Board and TikTok Inc. Board are recommended to meet (in-person or virtually) monthly. Following the first anniversary of the Operational Date, the TTUSDS Board and TikTok Inc. Board are recommended to meet quarterly.

**ARTICLE V**

**MANAGEMENT OF TTUSDS**

5.1 Key Management.

(1) Within seven (7) days following the appointment of the TTUSDS Board, TTUSDS shall ensure that the TTUSDS Board nominates individuals to serve as Key Management, and concurrently shall submit to the CMAs a list of such individuals, full internal organizational charts, and any other details reasonably requested by the CMAs for the CMAs to designate, in their sole discretion, any Personnel as Key Management. If the CMAs designate any Personnel of TTUSDS as Key Management, TTUSDS shall ensure that such Personnel are subject to the nomination, appointment, removal, and replacement processes for Key Management under Sections 5.1 and 5.2. TTUSDS shall ensure that all nominees for Key Management are Resident U.S. Citizens and hold no position within ByteDance or any of its Affiliates, in both cases for the duration of his or her service as Key Management and unless otherwise approved by the CMAs.

(2) The appointment of any individual as Key Management shall be subject to the prior non-objection of the CMAs. For each nominee, TTUSDS shall submit complete Personal Identifier Information, a *curriculum vitae* or similar professional synopsis, contact information, and any other information requested by the CMAs to ensure that the nominee can effectively perform the functions set forth in this Agreement. TTUSDS shall ensure that each nominee is available for an interview with the CMAs, at their request. If the CMAs do not object in writing within twenty-one (21) days following receipt of all necessary information about a nominee, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to one or more nominees, TTUSDS shall ensure that the TTUSDS Board nominates a different candidate within twenty-one (21) days following receipt of any such objection, subject to the same procedures as the initial nomination.

(3) TTUSDS shall ensure that the TTUSDS Board appoints each individual to serve as Key Management within three (3) days following the designation by or non-objection of the CMAs. TTUSDS shall ensure that each of the Key Management maintains his or her primary work location at a TTUSDS office location in the United States, that Key Management

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

are the senior officers with authority over the TikTok U.S. App and TikTok U.S. Platform in the United States, and that neither Key Management nor their subordinates report to any Personnel of ByteDance or its Affiliates.

5.2 Removal of Key Management. TTUSDS shall submit prior written notice to the CMAs before removing, replacing, or appointing any Key Management and shall not effect any such change in the event that the CMAs object in writing within fourteen (14) days following such notice; *provided, however*, that TTUSDS may immediately remove any Key Management for cause, subject to compliance with applicable law and the governance documents of TTUSDS, in which case TTUSDS shall notify the CMAs within one (1) day of such removal with an explanation of the cause. TTUSDS shall not remove any Key Management for his or her actual or attempted efforts to ensure compliance with this Agreement. TTUSDS shall ensure that the replacement and appointment of any Key Management are subject to the same process as the initial nomination and appointment process under Section 5.1.

5.3 Hiring Protocols.

(1) Existing ByteDance Personnel. The Transaction Parties shall notify the CMAs of any ByteDance or Affiliate Personnel, including a description of their job responsibilities, who (a) are not Resident U.S. Citizens and whose employment will be transferred from ByteDance or any of its Affiliates to TTUSDS, or (b) who may have Access to Protected Data under the Limited Access Protocol, no less than thirty (30) days prior to any such Personnel beginning to work for or support TTUSDS or having Access to Protected Data under the Limited Access Protocol, as relevant. The CMAs may, within twenty-one (21) days following receipt of such notification, object in writing to such Personnel, in which event TTUSDS shall not employ, independently engage the services of, or accept the transfer of employment contracts for such Personnel. For the avoidance of doubt, this provision does not apply to Key Management whose appointment, removal, and replacement shall follow the processes under Sections 5.1 and 5.2.

(2) Newly Hired Personnel. Within thirty (30) days following the Operational Date, TTUSDS shall develop and implement hiring protocols for onboarding newly hired Personnel (i.e., Personnel other than those originally transferred to or hired by TTUSDS as of the Operational Date) to TTUSDS. TTUSDS shall ensure that the hiring protocols provide for the vetting of whether the prospective Personnel is a CFIUS Restricted Person or has any current or prior employment, contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates for a period of one (1) year prior to his or her potential employment or support date. In the event that such a current or prior relationship exists, TTUSDS shall obtain the CMAs' prior written consent prior to hiring, onboarding, or granting or facilitating Physical Access to facilities or Logical Access to IT systems to such prospective Personnel. For the avoidance of doubt, this provision does not apply to Key Management whose appointment, removal, and replacement shall follow the processes under Sections 5.1 and 5.2.

(3) Reporting Lines. TTUSDS shall ensure that any Personnel transferred from ByteDance or any of its Affiliates to TTUSDS report solely to Key Management (or other



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

designated Personnel of TTUSDS) and do not report to any Personnel of ByteDance or its Affiliates, consistent with Section 5.1(3).

(4) Post-Separation. ByteDance shall not employ, independently engage the services of, or accept the transfer of employment contracts for any current or former employees of TTUSDS (including Key Management) for a period of one (1) year following the employee's separation from TTUSDS without the prior written consent of the CMAs. ByteDance shall ensure that none of its Affiliates, after conducting due diligence, knowingly employs, independently engages the services of, or accepts the transfer of employment contracts for any current or former employees of TTUSDS (including Key Management) for a period of one (1) year following the employee's separation from TTUSDS without the prior written consent of the CMAs except as approved in the Hiring Protocols.

(5) TTP Hiring.

TTUSDS shall ensure that the MSA requires the TTP to implement hiring protocols consistent with Subsection 5.4(2) for any prospective Personnel of the TTP who will perform services under the MSA, and TTUSDS shall enforce such requirement of the MSA against the TTP.

5.4 Content Advisory Council. Within sixty (60) days following the Operational Date, TTUSDS shall establish and maintain an external council of at least three (3) leading experts with experience in social media platforms, content moderation, free speech, or foreign influence who are Resident U.S. Citizens to advise TTUSDS on the Content Promotion and Filtering, Trust and Safety Moderation, and other content moderation policies for the TikTok U.S. App and TikTok U.S. Platform that are relevant to Trust and Safety Moderation (the "**Content Advisory Council**"). For the avoidance of doubt, the Content Advisory Council's role with respect to Content Promotion and Filtering, Trust and Safety Moderation, and other content moderation practices shall be advisory, not operational, and members of the current Content Advisory Council (established in March 2020) may serve on the Content Advisory Council under this Section 5.5. TTUSDS shall submit the name and a *curriculum vitae* or similar professional synopsis to the Third-Party Monitor and CMAs for each member of the Content Advisory Council, initially and upon any change to its composition. TTUSDS shall ensure that, at the Content Advisory Council's or CMAs' request, or at its own discretion, the Third-Party Monitor reviews human exclusions of content to ensure actions were taken consistent with Trust and Safety Moderation guidelines and delivers such reports to the Content Advisory Council upon completion. TTUSDS shall ensure that the Content Advisory Council may, as needed in its discretion, periodically engage with the Third-Party Monitor and CMAs about trends in foreign influence, propaganda, censorship, disinformation, and similar topics.

5.5 Communications Between Personnel of TTUSDS, ByteDance, and ByteDance Affiliates. Notwithstanding any other provision of this Agreement, communications between TTUSDS Personnel and Personnel of ByteDance or its Affiliates shall be permitted. Electronic communications between TTUSDS Personnel, on the one hand, and Personnel of ByteDance or its Affiliates, on the other hand, shall be logged for auditing purposes.

**ARTICLE VI**

**BYTEDANCE POC, COMPLIANCE OFFICER, AND SECURITY OFFICER**

6.1 Point of Contact. ByteDance shall at all times maintain a point of contact for the Third-Party Monitor and CMAs regarding ByteDance's compliance with this Agreement (the "**ByteDance POC**"). ByteDance shall notify the CMAs of the identity of the ByteDance POC within fourteen (14) days following the Effective Date, and within three (3) days following any change in the ByteDance POC.

6.2 Compliance Officer. TikTok Inc. shall at all times employ a compliance officer (the "**Compliance Officer**") who meets the qualifications set forth in Section 6.4, serves as the senior liaison between TikTok Inc. and the Third-Party Monitor and CMAs, and is responsible for overseeing compliance with this Agreement on behalf of TikTok Inc.

6.3 Security Officer. TTUSDS shall at all times employ a security officer (the "**Security Officer**") who meets the qualifications set forth in Section 6.4, serves as the senior liaison between TTUSDS and the Third-Party Monitor and CMAs, and is responsible for overseeing compliance with this Agreement on behalf of TTUSDS. TTUSDS shall ensure that the Security Officer reports directly and exclusively to the Security Committee.

6.4 Qualifications. TikTok Inc., with respect to the Compliance Officer, and TTUSDS, with respect to the Security Officer, shall ensure that the Compliance Officer and Security Officer:

- (1) are Resident Sole U.S. Citizens who have, or are eligible for, a U.S. personnel security clearance;
- (2) are qualified employees of TikTok Inc. or TTUSDS, respectively;
- (3) have sufficient and appropriate senior-level authority and resources within TikTok Inc. or TTUSDS, respectively, and the necessary technical skills and experience to ensure compliance with this Agreement and to fulfill all other obligations of the position;
- (4) have no current or prior contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates; *provided* that the initial Compliance Officer and Security Officer may be individuals who were previously employed in the United States by TikTok Inc. or ByteDance, Inc. as of the Effective Date and, in the case of the Security Officer, who will be transferred to TTUSDS by no later than the Operational Date; and
- (5) have Physical Access and Logical Access to all of the facilities, systems, records, and meetings of TikTok Inc. or TTUSDS, respectively, that in the sole discretion of the Third-Party Monitor and CMAs, are necessary to ensure compliance with this Agreement.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

The Compliance Officer and Security Officer may hold other titles and responsibilities at TikTok Inc. and TTUSDS, respectively; *provided* that such other responsibilities do not prevent the officer from performing his or her obligations in connection with the Agreement.

6.5 Nomination and Appointment. The appointment of the Compliance Officer and Security Officer shall be subject to the prior non-objection of the CMAs. Within fourteen (14) days following the Effective Date, the Transaction Parties shall nominate an initial Compliance Officer and initial Security Officer (in the case of the Security Officer, to be transferred to TTUSDS as of the Operational Date) and submit complete Personal Identifier Information, a *curriculum vitae* or similar professional synopsis, contact information, and any other information requested by the CMAs to assess whether the individual can effectively perform the obligations of the Compliance Officer or Security Officer, as applicable, under this Agreement. If the CMAs do not object in writing within twenty-one (21) days following receipt of all necessary information about the nominee, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object, the Transaction Parties shall nominate a different candidate within seven (7) days following receipt of any such objection, subject to the same procedures as the initial nomination. TikTok Inc. and TTUSDS, respectively, shall appoint the Compliance Officer and the Security Officer within three (3) days following non-objection by the CMAs.

6.6 Removal and Replacement.

(1) Neither TikTok Inc. nor TTUSDS shall remove any Compliance Officer or Security Officer without the prior non-objection of the CMAs. TikTok Inc. and TTUSDS, respectively, shall notify the CMAs at least fourteen (14) days before the proposed removal of a Compliance Officer or Security Officer unless such removal is for cause, and such removal shall only be proposed in conjunction with the nomination of a new candidate for the position, subject to the same procedures as the initial nomination. For the avoidance of doubt, such cause must consist of willful misconduct, gross negligence, reckless disregard, violation of applicable law, violation of company policy, or failure of the individual to perform his or her job duties. At no time shall TikTok Inc. or TTUSDS remove, penalize, or negatively change the terms of employment, including compensation and benefits, of the Compliance Officer or Security Officer for such officer's actual or attempted efforts to comply with or ensure compliance with this Agreement.

(2) Should the CMAs, in their sole discretion, determine that the Compliance Officer or Security Officer has failed to meet his or her respective obligations or has otherwise undermined the effectiveness of this Agreement, the CMAs may direct TikTok Inc. or TTUSDS, respectively, to remove the Compliance Officer or Security Officer, and TikTok Inc. or TTUSDS, respectively, shall promptly, and in any event within two (2) days, remove such officer.

(3) In the event of any vacancy in the Compliance Officer or Security Officer position, TikTok Inc. or TTUSDS, respectively, shall notify the CMAs within one (1) day and, within fourteen (14) days following such vacancy occurring, nominate a replacement Compliance Officer or Security Officer, subject to the same procedures as the initial nomination.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

During any vacancy of the Security Officer position, TTUSDS shall ensure that the chairman of the Security Committee fulfills the obligations of the Security Officer.

6.7 Communication with the Third-Party Monitor and CMAs. TikTok Inc. and TTUSDS shall ensure that the Compliance Officer and Security Officer, respectively, provide timely responses to inquiries from the Third-Party Monitor and CMAs about TikTok Inc.'s and TTUSDS's respective compliance with this Agreement. TikTok Inc. and TTUSDS shall ensure that the Compliance Officer and Security Officer, respectively, maintain availability for discussions with the Third-Party Monitor and CMAs on matters relating to compliance with this Agreement.

6.8 Reporting of Violations. TikTok Inc. and TTUSDS shall ensure that the Compliance Officer and Security Officer, respectively, report any actual or potential violation of this Agreement to the Third-Party Monitor and CMAs as soon as practicable, but in any event within one (1) day of learning of the actual or potential violation.

6.9 Costs. TikTok Inc. shall be responsible for all costs associated with the Compliance Officer and TTUSDS shall be responsible for all costs associated with the Security Officer.

6.10 Applicability Rule. Prior to the Operational Date, and unless otherwise specified in this Article VI, ByteDance and TikTok Inc. shall fulfill the requirements of this Article VI. Following the Operational Date, TTUSDS shall assume exclusive responsibility for the Security Officer.

## **ARTICLE VII**

### **LAWFUL U.S. PROCESS**

7.1 Lawful U.S. Process. TikTok Inc. and TTUSDS acknowledge their respective obligations to comply with valid Lawful U.S. Process. Without limiting such obligations, TikTok Inc. and TTUSDS agree that TTUSDS shall be principally responsible for complying with Lawful U.S. Process requests, whether directed at TikTok Inc. or TTUSDS, unless otherwise provided for in the Limited Access Protocol pursuant to Section 11.9. To this end, TTUSDS shall maintain policies relating to Lawful U.S. Process-related activities, regarding the security measures for handling, retaining, managing, and deleting information about Lawful U.S. Process-related activities. Those policies shall be subject to review by the Security Officer and approval by the Security Committee. No later than ninety (90) days after the Operational Date, TTUSDS shall deliver the Security Committee-approved policies relating to Lawful U.S. Process-related activities to the CMAs for their review and written approval. Subsequent changes to such policies also will be subject to the CMAs' written approval, excluding non-substantive revisions (e.g., typographical corrections).

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

**ARTICLE VIII**

**TRUSTED TECHNOLOGY PROVIDER**

8.1 Independence. At all times during any TTP's provision of services in connection with this Agreement, the Transaction Parties shall not have, and shall ensure that their respective Affiliates do not have, any financial or voting interest in, or otherwise possess an ability to Control, the TTP or its provision of services in connection with this Agreement, except to the extent necessary to enforce and ensure compliance with the MSA executed following the non-objection of the CMAs. The Transaction Parties shall treat the TTP as an arm's-length commercial vendor, and none of the Transaction Parties shall engage in any transaction following the Effective Date through which the TTP gains an equity interest in, or any governance rights with respect to, any of the Transaction Parties.

8.2 Master Services Agreement.

(1) Within forty five (45) days following the Effective Date, the Transaction Parties shall, in coordination with the TTP, submit an initial draft MSA to the CMAs. The MSA, including any amendments thereto, shall be subject to the prior non-objection of the CMAs. The Transaction Parties, in coordination with the TTP, shall subsequently submit a draft of the MSA, and any amendments thereto, to the CMAs, and resolve any concerns raised by the CMAs to the CMAs' satisfaction prior to the execution of the MSA or any amendment thereto. If the CMAs do not object in writing within forty-five (45) days following receipt of a draft MSA or amendment, the lack of action shall constitute a non-objection. The Transaction Parties shall execute the MSA or any amendment thereto within three (3) days following the non-objection of the CMAs (if executed prior to the Operational Date, the Transaction Party shall ensure that TTUSDS joins as a party to the MSA by no later than the Operational Date). The Transaction Parties shall submit a copy of the final MSA and any amendment thereto to the CMAs within three (3) days following execution. In the event that Oracle (or a successor TTP) is replaced as the TTP, the Transaction Parties shall execute an MSA with the replacement TTP following the non-objection of the CMAs to the replacement TTP under Section 8.2(6), in accordance with the procedures and requirements for the initial MSA.

(2) The Transaction Parties shall ensure that the MSA incorporates all of the provisions applicable to the TTP, Protected Data, Source Code and Related Files, Recommendation Engine, and the TikTok U.S. App and TikTok U.S. Platform under this Agreement, and further incorporates the obligations of the Transaction Parties under this Agreement to ensure that the TTP takes the actions specified in this Agreement and that TTUSDS fully cooperates with the TTP to ensure that the TTP can take such actions as specified in this Agreement, in all cases to the CMAs' satisfaction in their sole discretion.

(3) The Transaction Parties shall ensure the TTP receives all submissions of findings arising from the public bug bounty program for the TikTok U.S. App.

(4) The Transaction Parties shall ensure that the MSA sets forth specific commitments by TTUSDS and Oracle (or a successor TTP), including submitting to oversight

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

and auditing by the CMAs and third parties designated under this Agreement of services performed under the MSA. The Transaction Parties shall ensure the MSA grants the TTP the right, in its sole discretion, to seek the views of the Third-Party Monitor and CMAs in the event of any disagreement between the Transaction Parties and the TTP regarding the security of Protected Data and Source Code and Related Files.

(5) The Transaction Parties shall amend the MSA upon written direction from the CMAs, in their sole discretion; *provided* that any amendments to the MSA initiated by the CMAs shall be for purposes of ensuring compliance with this Agreement and after consultation with the Transaction Parties, the TTP, and the Third-Party Monitor.

(6) The Transaction Parties may, solely based on evidence that the TTP has failed to comply with the material terms of the MSA and with notice to the CMAs regarding the provision(s) breached and supporting evidence, request that the CMAs permit the Transaction Parties to remove the TTP for cause. The Transaction Parties shall not remove the TTP without the prior written consent of the CMAs. The CMAs, in their sole discretion, may require the Transaction Parties to remove and replace the TTP. The Transaction Parties shall ensure that the MSA provides for a process to effectively transition responsibilities in connection with this Agreement to a new TTP in the event of a removal or replacement. Within thirty (30) days following any vacancy in the TTP position, the Transaction Parties shall submit for the prior non-objection of the CMAs the name and any additional information requested by the CMAs of a proposed vendor to serve as the TTP. If the CMAs object, the Transaction Parties shall not engage the vendor and shall submit another proposed vendor to the CMAs within thirty (30) days following receipt of the CMAs' objection. If the CMAs do not object within thirty (30) days following receipt of all necessary information regarding a proposed replacement TTP, the lack of action shall constitute a non-objection.

(7) The Transaction Parties shall provide sufficient financial resources, consistent with industry-standard rates for comparable services and determined in coordination with the TTP, to enable the TTP to fully perform the responsibilities designated to the TTP in connection with this Agreement and under the MSA. The Transaction Parties shall ensure that the MSA requires the TTP to promptly notify the CMAs if the TTP believes, in its sole discretion that it lacks sufficient funding or related resources under the MSA to adequately conduct the tasks required of it under the MSA and in connection with this Agreement. The Transaction Parties shall provide semi-annual updates to the Third-Party Monitor and CMAs regarding the budgeting and funding of the TTP under the MSA and in connection with this Agreement.

8.3 Rule of Construction. Any provision of this Agreement that requires any Transaction Party, individually or collectively, to ensure that the TTP takes a specified action shall be deemed to require the applicable Transaction Party to enforce, contractually through the MSA, the TTP's fulfillment of and compliance with its obligations in connection with this Agreement.

8.4 TikTok U.S. Platform Deployment. By no later than the Operational Date, the Transaction Parties shall, in coordination with the TTP, take all steps necessary to facilitate TTUSDS's initial deployment of the TikTok U.S. Platform in the TTP's secure cloud

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

infrastructure in the United States, which shall be logically separate from the DTC, and thereafter the Transaction Parties shall ensure that TTUSDS continues to maintain and operate the TikTok U.S. Platform exclusively in the TTP's secure cloud infrastructure in the United States, except as otherwise provided in this Agreement (including with respect to CDNs). The Transaction Parties shall ensure that TTUSDS's deployment of the TikTok U.S. Platform includes the creation of secure testing, build, integration, and deployment environments for the TikTok U.S. App and TikTok U.S. Platform that are permissioned and auditable. The Transaction Parties shall ensure the TTP implements processes and controls to monitor these environments to ensure compliance with this Agreement related to Source Code and Related Files and Logical Access to Protected Data.

8.5 Content Delivery Networks. TTUSDS shall not be required to maintain and operate CDNs solely within the TTP's secure cloud infrastructure; *provided* that TTUSDS shall maintain, operate, and contract for any CDN that is not within the TTP's secure cloud infrastructure in accordance with the following requirements:

(1) Commercial CDNs: TTUSDS shall ensure that the use of any third-party CDN providers for the TikTok U.S. Platform complies with the vendor approval requirements, including the Vendor Program Policy pursuant to Article XIII of this Agreement.

(i) TTUSDS shall ensure that all such CDN servers utilized for the delivery of content in the United States reside exclusively in the United States.

(ii) TTUSDS shall consult with the TTP and Third-Party Monitor on configuration changes related to a CDN. All such changes shall be logged in auditable fashion, with the logs made available to the Third-Party Monitor, the Third-Party Auditor, and the CMAs. TTUSDS shall involve the TTP in any discussions or work with the third-party CDN provider related to such configuration changes.

(iii) TTUSDS shall ensure that the TTP has the ability to monitor and audit configuration changes related to CDNs through a gateway in the TTP's secure cloud infrastructure for Access to the CDN network elements or the built-in capability provided by the commercial CDN. TTUSDS shall ensure that the gateway or built-in capability of the commercial CDN includes an alert system that notifies both TTUSDS and the TTP of any change of origin settings or that otherwise results in unexpected traffic routing patterns.

(2) Proprietary CDNs.

(i) All Source Code and Related Files for any proprietary CDN servers maintained by TTUSDS shall be subject to the applicable software assurance requirements of Article IX, including review and testing by the TTP in parallel with deployment of Executable Code.

(ii) TTUSDS shall work with the TTP to develop technical means that enable (a) the TTP to monitor the interaction of the servers with the other elements of the

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

TikTok U.S. Platform and systems operated by or on behalf of ByteDance serving non-TikTok U.S. Users, and (b) the TTP to block any such interactions that are unexpected or unauthorized and report, within one (1) day of discovery and validation, any such interactions to the Third-Party Monitor and CMAs.

(iii) Any proprietary CDN servers maintained by TTUSDS shall not Access any Protected Data other than IP addresses, which TTUSDS shall ensure are masked when stored on the CDN server, unless TTUSDS requests, and the CMAs approve, Access by the CDN to any other Protected Data.

(iv) On an annual basis, TTUSDS shall, with input from the TTP and Third-Party Monitor, reevaluate and report to the CMAs regarding the feasibility of third-party vendors adequately supporting services covered by proprietary CDNs. When TTUSDS concludes that third-party vendors can adequately support the services provided by proprietary CDNs consistent with industry-standard rates for comparable services, TTUSDS shall transition those services to a third-party vendor on a timeline established in consultation with the TTP, Third-Party Monitor, and CMAs.

(3) For the avoidance of doubt, neither ByteDance nor any of its Affiliates shall have Access to the CDNs supporting the TikTok U.S. Platform.

8.6 Diagrams. By no later than thirty (30) days prior to the Operational Date, and thereafter within fourteen (14) days following a request from the CMAs, the Transaction Parties shall submit, and shall ensure the TTP submits, respectively as applicable to their individual obligations or collectively as appropriate, Architecture Diagrams, Data Flow Diagrams, Existing Network Diagrams, and Source Code Review Diagrams for the TikTok U.S. Platform to the Third-Party Monitor and CMAs. The Transaction Parties shall promptly respond, and shall ensure the TTP promptly responds, to inquiries from the Third-Party Monitor and CMAs for further or clarifying information regarding any submission of Architecture Diagrams, Data Flow Diagrams, Existing Network Diagrams, and Source Code Review Diagrams.

## ARTICLE IX

### DEDICATED TRANSPARENCY CENTER AND SOURCE CODE SECURITY

9.1 DTC Locations and Protocols. The Transaction Parties shall mutually develop with the TTP the locations and Physical Access and Logical Access procedures of the DTC, as well as the security requirements, infrastructure, technical and architectural parameters, and equipment to be used within the DTC (together, the “**DTC Operating Protocols**”). The Transaction Parties shall ensure that the DTC is located at all times in the United States; *except that* supporting DTCs may be located in the United Kingdom, Australia, New Zealand, and Canada (the “**DTC Approved Countries**”). The Transaction Parties shall at all times comply with the DTC Operating Protocols (as amended from time to time, at the request of the Transaction Parties or TTP, or at the direction of the CMAs). The Transaction Parties shall not amend the DTC Operating Protocols without the prior written consent of the TTP.



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(1) The DTC Operating Protocols and any amendments thereto shall be subject to the prior non-objection of the CMAs. The Transaction Parties shall submit the DTC Operating Protocols to the CMAs within seven (7) days following the Effective Date. The Transaction Parties shall submit written confirmation to the CMAs of the TTP's agreement to the initial DTC Operating Protocols and any amendment thereto. If the CMAs do not object in writing within fourteen (14) days following receipt of the DTC Operating Protocols or any amendment thereto, the lack of action shall constitute a non-objection. If the CMAs object, the Transaction Parties shall fully resolve the CMAs' concerns to the satisfaction of the CMAs in their sole discretion before implementing the DTC Operating Protocols or any amendment thereto. The Transaction Parties shall adopt and implement the DTC Operating Protocols with the TTP following the non-objection of the CMAs and by no later than the Operational Date.

(2) The Transaction Parties shall not, and shall ensure that their respective Affiliates do not, Access or use the DTC except in accordance with the DTC Operating Protocols.

9.2 Provision of Source Code and Related Files via the DTC.

(1) ByteDance shall provide, and shall ensure that its Affiliates provide, all current and future Source Code and Related Files to the TTP and the Source Code Inspector via the DTC for the purposes of software assurance and secure deployment of the TikTok U.S. App and TikTok U.S. Platform, as well as the performance of all related services under the MSA. ByteDance shall initially provide, and shall ensure that its Affiliates provide, all current Source Code and Related Files to the TTP via the DTC by no later than the Operational Date and on an ongoing basis thereafter. The transfer of Source Code and Related Files to the TTP via the DTC shall not be deemed to transfer any title that ByteDance or any of its Affiliates has in the Source Code and Related Files.

(2) In connection with its provision of all current and future Source Code and Related Files to the TTP via the DTC, ByteDance shall produce a software bill of materials (the "SBOM") or its equivalent, that inventories, for each version of the Source Code and Related Files, all components and their origin, including sufficient data for the TTP to verify each component and to cross-reference with known vulnerabilities. The Transaction Parties shall ensure the TTP, through signature verification (to the extent possible), verifies that the software versions and other components identified in the SBOM or its equivalent matches the Source Code and Related Files where source code is available (e.g., third-party libraries), and any third-party software, including for any build artifacts that are incorporated into the TikTok U.S. App or the TikTok U.S. Platform by reference to software repositories. The Transaction Parties shall also ensure the TTP verifies, to the extent that it determines necessary and feasible, third-party software where the source code is not available (e.g., commercial-off-the-shelf software and open source tools).

(3) The Transaction Parties shall designate Personnel who are based in the United States, Australia, New Zealand, Canada, and the United Kingdom, unless otherwise approved in writing by the CMAs, as primary points of contact with the TTP and the CMAs for requirements related to the DTC and Source Code and Related Files.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

9.3 DTC Access.

(1) ByteDance shall not withhold, and shall ensure that none of its Affiliates withhold, Physical Access to the DTC without just cause (e.g., for the protection of its intellectual property) and on terms consistent with the MSA and this Agreement. ByteDance shall ensure that all Persons designated in writing by the CMAs, in their sole discretion, have Access to the DTC. Any Person designated by the CMAs pursuant to this section shall treat all information such Person observes or has Access to as confidential information consistent with 31 C.F.R. § 800.802.

(2) ByteDance shall ensure that any confidentiality requirements for Access to the DTC do not impede the ability of the Third-Party Monitor or the CMAs to conduct monitoring pursuant to this Agreement.

(3) ByteDance shall grant, and shall ensure that its Affiliates grant, all Personnel of TTUSDS, the TTP, the Source Code Inspector, and the Third-Party Monitor Physical Access to the DTC, consistent with the DTC Operating Protocols. ByteDance shall ensure that such Personnel have a constant and consistent right and ability to have Physical Access to the DTC. ByteDance shall not take, and shall ensure that none of its Affiliates take, any action to delay or prevent Physical Access to the DTC by Personnel of TTUSDS, the TTP, the Source Code Inspector, or the Third-Party Monitor. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.3(3) to the Third-Party Monitor and CMAs.

(4) ByteDance shall grant, and shall ensure that its Affiliates grant, Personnel of TTUSDS and the TTP full Logical Access to, and the practical ability to review and inspect, all Source Code and Related Files in the DTC, consistent with the licensing terms under Section 2.5 (including any confidentiality terms) and this Agreement, without any interference by ByteDance. ByteDance may maintain monitoring within the DTC to the extent necessary to protect its intellectual property; *provided* that such monitoring shall not impede or compromise the integrity of the TTP's confidential inspection of Source Code and Related Files. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.3(4) to the Third-Party Monitor and CMAs.

9.4 Source Code and Related Files Location. ByteDance may require in the DTC Operating Protocols that the TTP Personnel shall not review or inspect Source Code and Related Files other than via the DTC and that the Source Code and Related Files be used solely for the purposes required under this Agreement. ByteDance shall ensure that at least one (1) location of the DTC is within the facilities of the TTP. TTUSDS shall ensure the TTP maintains Logical Access to Source Code and Related Files via the DTC, consistent with the DTC Operating Protocols, to conduct automated and manual review of Source Code and Related Files.

9.5 Software Assurance Process. As part of the software assurance process, the Transaction Parties shall ensure that the Source Code and Related Files and Executable Code do not include Malicious Code.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

9.6 Vulnerability Reporting. TTUSDS shall report promptly, and shall ensure the TTP reports promptly, via a format mutually acceptable to the CMAs and TTUSDS, and in any event within one (1) business day of discovery and validation, any findings of zero day vulnerabilities designated by the TTP as at least high severity or equivalent (following consultation with TTUSDS and based on recognized criteria such as the Common Vulnerability Scoring System and the TTP's judgment regarding whether the vulnerabilities are exploitable) or any instance of Malicious Code in the Source Code and Related Files or Executable Code to ByteDance, the Third-Party Monitor, and the CMAs, subject to the following:

(1) In the event that the TTP discovers what it believes to be, in its sole discretion, the presence of Malicious Code in the Source Code and Related Files or Executable Code, TTUSDS shall ensure the TTP submits the written report directly to the CMAs and Third-Party Monitor prior to notifying ByteDance, and, at the direction of the CMAs, provide a copy to ByteDance soon thereafter in which the TTP may redact information, in its sole discretion or at the direction of the CMAs.

(2) The Transaction Parties shall not disclose, and shall ensure the TTP does not disclose, to the public any findings of zero days, vulnerabilities, or Malicious Code in the Source Code and Related Files or Executable Code discovered by the TTP or the Transaction Parties unless:

(i) they are required to do so by applicable law or regulation or in relation to a judicial or administrative proceeding;

(ii) there is no disagreement among ByteDance, TTUSDS, and the TTP regarding the findings; or

(iii) in the event that there is such a disagreement among ByteDance, TTUSDS, and the TTP, TTUSDS or the TTP determines, after consultation with the Security Committee, that disclosure is merited given industry practices on responsible disclosure, such as the International Organization for Standardization ("ISO") 29147 Standard.

(3) TTUSDS shall ensure that the timing and contents of any public disclosure pursuant to this Section are consistent with industry practices on responsible disclosure, such as the ISO 29147 standard, to ensure that the zero day, vulnerability, or Malicious Code is remediated or otherwise patched prior to disclosure, and that the disclosure does not lead to exploitation of the zero day, vulnerability, or Malicious Code.

(4) TTUSDS shall ensure that any public disclosure of a zero day, vulnerability, or Malicious Code is first notified to the other Transaction Parties, the TTP, the Security Committee, the Third-Party Monitor, and the CMAs. The Transaction Parties shall not disclose, shall ensure the TTP and the Third-Party Monitor do not disclose, and shall ensure that the Security Committee does not disclose, any zero day, vulnerability, or Malicious Code that is so pre-notified to them, until after it is made public by TTUSDS or the TTP consistent with this

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Section 9.6(4), and the Transaction Parties shall ensure that any such disclosure is limited to the content made public by TTUSDS or the TTP.

9.7 Source Code and Related Files Review Process. Upon receiving Source Code and Related Files via the DTC, initially and for any subsequent change, TTUSDS shall ensure the TTP deploys, immediately and on an ongoing basis, a team of engineers to examine all aspects of the Source Code and Related Files using all tools required in the TTP's sole discretion, including both automated tools and human inspection, to assess the presence of any zero days, vulnerabilities, or Malicious Code, that could affect the confidentiality, integrity, or availability of the TikTok U.S. App, TikTok U.S. Platform, or Protected Data. The Transaction Parties shall permit, and shall ensure that their respective Affiliates permit, use by the TTP of all tools necessary to perform the obligations in connection with this Agreement.

9.8 TikTok U.S. App Mobile Security Measures. Within sixty (60) days following the Operational Date, or as otherwise extended by the CMAs, TTUSDS shall submit to the CMAs protocols developed with the TTP that ensure the TTP creates protections to ensure that the TikTok U.S. App cannot Access or transmit Protected Data in an unauthorized manner or exploit the mobile devices of TikTok U.S. Users (the "**Security Protocols**"). TTUSDS shall ensure that the protections are effective no later than one hundred and twenty (120) days following the Operational Date, unless otherwise extended by the CMAs. TTUSDS shall ensure the TTP agrees, in writing, with the extent and scope of the security measures in the initial protocols for each of the different apps comprising the TikTok U.S. App. For the iOS and Android mobile apps, the initial protocols shall include measures such as: activation logic to enable the mobile security measures for all TikTok U.S. Users; rules-based interceptors to analyze and, if necessary, block data flows; auditing and logging of application behavior to alert the TTP of any issues; and configuration services to enable the TTP to adjust the mobile sandbox as needed in its sole discretion. Within seven (7) days following the implementation of the Security Protocols, ByteDance shall ensure that all TikTok U.S. Users must download or update to the version of the TikTok U.S. App that includes the protections of the Security Protocols (e.g., that includes the mobile security measures to use the TikTok U.S. App). TTUSDS shall ensure the TTP submits monthly reports to the Third-Party Monitor and CMAs on its progress implementing the mobile security measures. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with the Security Protocols to the Third-Party Monitor and CMAs.

9.9 Initial Source Code and Related Files Inspection.

(1) Within one hundred and eighty (180) days following the Operational Date, or as otherwise extended by the CMAs, TTUSDS shall ensure the TTP completes the initial inspection of Source Code and Related Files pursuant to Section 9.7 (the "**Initial Inspection**"), with the timing (other than the due date) and manner of the Initial Inspection determined by the TTP in its sole discretion. TTUSDS shall ensure the TTP submits to the Third-Party Monitor and CMAs no later than three (3) days following the completion of the Initial Inspection a certification of completion of the Initial Inspection, which shall include a summary of the findings of the Initial Inspection and no later than ten (10) days following the completion of the Initial Inspection a plan and timeline for any resulting remediations to the Source Code and

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Related Files requested of or made by ByteDance as a result of the Initial Inspection. TTUSDS shall ensure the TTP submits monthly reports to the Third-Party Monitor and CMAs on its progress completing the Initial Inspection.

(2) During the Initial Inspection, ByteDance and its Affiliates may continue to update the Source Code and Related Files or subsets thereof; *provided, however*, that ByteDance shall ensure that any such updates do not impede the Initial Inspection and are clearly identifiable as updates upon inspection by the TTP. Prior to the deployment of any updates to the Source Code and Related Files prior to the completion of the Initial Inspection, ByteDance shall consult with TTUSDS and the TTP regarding the impact of any such updates on the Initial Inspection and, where in the TTP's sole discretion such updates will impede the timely completion of the Initial Inspection, ByteDance shall not make, and shall ensure that none of its Affiliates make, such updates. TTUSDS shall ensure the TTP reports ByteDance's or its Affiliates' failure to refrain from updating the Source Code and Related Files as required by this Section 9.9(2) to the Third-Party Monitor and CMAs and includes any updates to the Source Code and Related Files in the Initial Inspection, with the Initial Inspection considered incomplete until all updates are evaluated.

9.10 Prohibition on Deployment without TTP Security Processes.

(1) The Transaction Parties shall not deploy, and shall ensure that none of their respective Affiliates deploys, to the TikTok U.S. App or TikTok U.S. Platform any changes, updates, alterations, or improvements to the Source Code and Related Files that are not subject to security review and inspection by the TTP. For changes, updates, alterations, or improvements to the Source Code and Related Files for the TikTok U.S. App, the Transaction Parties shall ensure the TTP completes its inspection before such updates are deployed, and made available to TikTok U.S. Users. For changes, updates, alterations, or improvements to the Source Code and Related Files for the TikTok U.S. Platform, the Transaction Parties shall ensure the TTP conducts its inspection asynchronously in accordance with the Software Assurance Protocols but no later than thirty (30) days following deployment. The Transaction Parties shall ensure that only Source Code and Related Files for which the SBOM or its equivalent has been digitally signed by the TTP is deployed to the TikTok U.S. Platform. The Transaction Parties shall further ensure that any executable files derived from the Source Code and Related Files and deployed on the TikTok U.S. Platform are compiled exclusively within the TTP's secure cloud infrastructure. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.10(1) to the Third-Party Monitor and CMAs.

(2) ByteDance shall address, and shall ensure that its Affiliates address, all issues with the Source Code and Related Files to the satisfaction of TTUSDS and the TTP, in their sole discretion. In the event of a disagreement between TTUSDS and the TTP regarding the security of the Source Code and Related Files, the view of the Security Committee shall prevail; *provided* that should the TTP seek the view of the CMAs in the event of a disagreement with the Security Committee, the view of the CMAs shall prevail. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.10(2) to the Third-Party Monitor and CMAs.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(3) In all cases, the Transaction Parties shall ensure the TTP determines, in its sole discretion, when its security review and inspection pursuant to this Section 9.10 is complete.

(i) If at any time there are insufficient funds or time for the TTP to fulfill its obligations, TTUSDS shall ensure the TTP immediately informs ByteDance and the Third-Party Monitor of the insufficiency. If, upon notification of a perceived funding insufficiency, the Security Committee determines unanimously that the TTP's request is inconsistent with industry-standard rates for comparable services, TTUSDS and the TTP shall resolve the disagreement consistent with the terms of the MSA and the timelines under Section 9.10(3)(ii) shall be tolled during such resolution. For the avoidance of doubt, tolling under this Section 9.10(3)(i) shall not affect the requirement that all changes, updates, alterations, or improvements to the Source Code and Related Files must undergo security review and inspection by the TTP consistent with Section 9.10(1), including the requirement that any such changes to the Source Code and Related Files for the TikTok U.S. App be reviewed and inspected prior to deployment to TikTok U.S. Users.

(ii) ByteDance shall resolve any insufficiency of funding or time within fifteen (15) days of receipt of the notice under Section 9.10(3)(i). If such funding or timing insufficiency is not resolved within five (5) days, TTUSDS shall ensure the TTP immediately reports such insufficiency to the Third-Party Monitor and CMAs.

9.11 Source Code Inspector.

(1) The Transaction Parties shall engage a third-party selected by TTUSDS and the TTP to serve as an independent inspector (the "**Source Code Inspector**") of the Source Code and Related Files in the DTC. The engagement of the Source Code Inspector shall be subject to the prior non-objection of the CMAs. The Transaction Parties shall submit for the CMAs' review a proposed Source Code Inspector within sixty (60) days following the Operational Date. If the CMAs object, the Transaction Parties shall submit another proposed candidate for the CMAs' review within thirty (30) days following receipt of the objection. If the CMAs do not object within fourteen (14) days following receipt of all necessary information about a candidate, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. The Transaction Parties shall annually place funds in escrow to retain the Source Code Inspector. The Transaction Parties shall ensure that the CMAs are third-party beneficiaries of their agreement with the Source Code Inspector.

(2) The Transaction Parties shall ensure that the Source Code Inspector is granted all Physical Access and Logical Access necessary to conduct a security vulnerability assessment within the DTC pursuant to protocols approved in advance by the CMAs and submits reports directly to the CMAs and Third-Party Monitor, with a copy to the Transaction Parties and the TTP, on a schedule determined by the CMAs.

(3) The Transaction Parties shall ensure that the Source Code Inspector submits quarterly reports to the Transaction Parties, the TTP, and the Third-Party Monitor detailing any findings of concern, or if none, stating so. The Transaction Parties shall submit a

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

copy of any such report to the CMAs within three (3) days following a request by the CMAs. The CMAs may, in their sole discretion, change the frequency of the Source Code Inspector's reporting obligations.

(4) The Transaction Parties, in coordination with the TTP, shall promptly address all findings of concern identified by the Source Code Inspector.

9.12 Source Code Lifecycle.

(1) ByteDance shall develop the Source Code and Related Files and provide a mirror repository of it to the TTP, including the SBOM or its equivalent, via the DTC such that the TTP can at all times maintain full and simultaneous visibility into the Source Code and Related Files and any changes thereto via the DTC. Any changes, updates, alterations, or improvements to the Source Code and Related Files must: (i) for the TikTok U.S. App, be batched in logical collections according to a regular release schedule (except for time-sensitive changes, updates, alterations, or improvements); and (ii) for the TikTok U.S. App and TikTok U.S. Platform, only use build artifacts, whether proprietary or third-party build artifacts, from a repository within the TTP's secure cloud infrastructure and to be included in the SBOM or its equivalent.

(2) The Transaction Parties shall meet regularly, and no less than quarterly, with the TTP and Third-Party Monitor to discuss planned changes, updates, alterations, or improvements to the Source Code and Related Files for the TikTok U.S. App and TikTok U.S. Platform, including new features, functionality, and other product roadmaps, and their implications for security and the TTP's assurance processes and responsibilities.

(3) Only TTUSDS and the TTP shall compile the Source Code and Related Files. Once compiled, TTUSDS and the TTP shall generate the SBOM for the code they have respectively compiled, and the TTP shall digitally sign each such SBOM, exclusively via the DTC.

(4) TTUSDS and the TTP shall only deploy Executable Code to the TikTok U.S. App and TikTok U.S. Platform in compliance with the security review and inspection requirements of Section 9.10 and may remove Executable Code from the DTC for that purpose.

(5) The Transaction Parties shall ensure that the DTC affords the TTP and TTUSDS an end-to-end secure deployment system established by the TTP and TTUSDS for the deployment of the TikTok U.S. App and TikTok U.S. Platform, respectively, that implements the following operations with respect to Source Code and Related Files:

(i) Any Source Code and Related Files shall not be deployed to the TikTok U.S. App and TikTok U.S. Platform unless it is subject to the security review and inspection protocols of the TTP pursuant to Section 9.10;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(ii) TTUSDS and the TTP shall have the ability to securely monitor and inspect the end-to-end Source Code and Related Files deployment lifecycle to ensure the integrity of the chain of custody; and

(iii) Source Code and Related Files shall not be removed from the DTC.

9.13 Recommendation Engine and Content Moderation Processes.

(1) On or before the Operational Date, TTUSDS shall provide to the Content Advisory Council, the TTP, and the Third-Party Monitor a copy of the U.S. playbook for human moderators, which shall be subject to approval by the Security Committee. Subsequently, TTUSDS shall provide an updated copy of this playbook to the Content Advisory Council and Security Committee any time changes are made to it. An updated copy shall also be provided to the Third-Party Monitor, the TTP, and the CMAs upon request.

(2) Within sixty (60) days following the Operational Date:

(i) The Transaction Parties shall ensure the TTP begins conducting periodic software inspection and testing of the Software and associated data implementing the Recommendation Engine to ensure that its machine-implemented rules and algorithms conform to the documentation provided to the TTP by TTUSDS and that the Software and data associated with Content Promotion and Filtering and Trust and Safety Moderation systems (together, "**Content Moderation Processes**") also conform to the published policies for the TikTok U.S. App. TTUSDS shall ensure that the Recommendation Engine is trained exclusively within the TTP's secure cloud infrastructure.

(ii) If the TTP or the Third-Party Monitor determine that the documentation and policies described in Section 9.13(1)(i) are insufficient to support the inspections and reviews described in this Section 9.13, then either the TTP or the TPM may inform TTUSDS and TTUSDS shall promptly deliver supplementary documentation. TTUSDS shall update the documentation described in this Section 9.13 from time to time as the Recommendation Engine, and Content Moderation Processes evolve.

(iii) The TTP and TPM shall report any findings under this Section 9.13(2) to the Security Committee on an ongoing basis, including any findings of material inconsistencies between the Recommendation Engine and the Content Moderation Processes and the related documentation and policies within one (1) day of discovery and validation. Upon receipt of a report from the TTP, the Security Committee and TPM, in consultation with the TTP and Content Advisory Council, shall evaluate and determine whether results of the inspection and testing of the source code implementing the Recommendation Engine and Content Moderation Processes are not operating in material conformance with the documentation and policies ("**Adverse Findings**"). For the avoidance of doubt, it is understood that the operation of the Recommendation Engine



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

and Content Moderation Processes in conformance with related documentation and policies may result in diverse content being published via the TikTok U.S. App because of the nature of the underlying machine learning technologies and not because of inconsistencies between the operation of the Software and the related documentation and policies and so Adverse Findings shall not be based solely on outcome-based evidence.

(iv) At the request of the Security Committee, the CMAs, or the TTP, the Third-Party Auditor shall conduct an audit of the Content Moderation Processes' implementation for consistency with approved Content Moderation Processes policies and guidelines.

(v) In the event of an Adverse Finding, ByteDance shall, in consultation with TTUSDS and the TTP, as appropriate and necessary, promptly implement any necessary changes or updates to the Software implementing the Recommendation Engine and Content Moderation Processes, as applicable, to the extent necessary to address such findings. If ByteDance is unable or unwilling to do so the CMAs shall, in consultation with TTUSDS, the Content Advisory Council, and the Security Committee, determine whether—contrary to ByteDance's conclusion—a remediation plan is feasible within a reasonable period of time.

(1) If on the basis of the consultation required by the prior paragraph the CMAs determine:

(X) it is not feasible within a reasonable period of time for a remediation plan to be implemented; or

(Y) ByteDance, in consultation with TTUSDS and the TTP, as appropriate and necessary, fails to implement any necessary changes or updates required by the remediation plan to the Software implementing the Recommendation Engine and Content Moderation Processes, as applicable,

then the CMAs may make the Adverse Findings public following the process described in this section and after first consulting with the Security Committee regarding the content of any such public statement and providing ByteDance with the opportunity to review and provide comments on the content of the statement at least two (2) days prior to release of the public statement.

9.14 Further Testing of Source Code and Related Files. At the request of the CMAs in their sole discretion, ByteDance shall promptly allow the TTP to conduct security testing (e.g., static or dynamic testing or other generally accepted practices) of Source Code and Related Files and Executable Code via the DTC to ensure the security of the Source Code and Related Files and Executable Code.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

9.15 Source Code and Related Files Alterations.

(1) ByteDance shall retain the exclusive right to alter the Source Code and Related Files, subject to the requirements and prohibitions in this Agreement.

(2) ByteDance shall promptly alter the Source Code and Related Files at the request of TTUSDS, the TTP, the Third-Party Monitor, or the CMAs, to ensure compliance with this Agreement, and shall submit a response and initial implementation plan to TTUSDS and the TTP within three (3) days of receipt of any such request, subject to the following:

(i) If ByteDance rejects such a request, ByteDance shall submit the rejection and its rationale in writing to the TTP, the Security Committee, the Third-Party Monitor, and the CMAs promptly and, in any event, within one (1) day of the rejection;

(ii) If ByteDance rejects such a request to alter the Source Code and Related Files, fails to alter the Source Code and Related Files as requested in a timely manner and consistent with the implementation plan, or fails to respond to the requested alteration within three (3) days, TTUSDS shall ensure the TTP, in coordination with the Third-Party Monitor, evaluates practicable options to ensure compliance with this Agreement absent the requested alteration. If after due consideration of all options, the TTP determines that there is no adequate option to ensure compliance with this Agreement without the requested Source Code and Related Files alteration, TTUSDS shall ensure the TTP, in consultation with the Security Committee, notifies ByteDance (the "**Suspension Notice**"), with a copy to the CMAs, the Third-Party Monitor, and the Security Committee, of the TTP's intent to suspend user access to the TikTok U.S. Platform, in whole or in part, in no less than two (2) days and no more than four (4) days (the period between the date of the notice and the suspension, the "**Remediation Window**"). TTUSDS shall ensure the TTP implements any suspension as set forth in a Suspension Notice upon expiration of the Remediation Window unless: (a) ByteDance has remediated the issue to the TTP's satisfaction in its sole discretion; (b) ByteDance has obtained a waiver from the CMAs; or (c) a majority of the Security Committee has determined and certified to the CMAs that the suspension is not necessary to ensure the Transaction Parties' compliance with this Agreement, accompanied by a reasoned and detailed analysis and explanation for the decision;

(iii) At the request of the CMAs, TTUSDS shall ensure the TTP submits to the CMAs a confidential report regarding any rejected request pursuant to this Section 9.15, as well as any Security Committee override of a suspension; and

(iv) If a suspension is implemented, once ByteDance provides Source Code and Related Files alterations to address the identified issue, TTUSDS shall ensure the TTP promptly reviews ByteDance's Source Code and Related Files alterations and, if acceptable to the TTP in its sole discretion, immediately reinstates user access to the TikTok U.S. Platform.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

9.16 Location-Based Source Code Changes. Within thirty (30) days following the Operational Date, the Transaction Parties, in coordination with the TTP, shall, if necessary, update the Source Code and Related Files to reasonably ensure that TikTok U.S. Users physically located in the United States are restricted to the fullest extent possible from manipulating their geographic location within any version of the TikTok Global App to a country other than the United States, such that TikTok U.S. Users may solely use the TikTok U.S. App maintained and operated by the TTP. The Transaction Parties shall not take any action to degrade the user experience of TikTok U.S. Users in a manner designed to encourage TikTok U.S. Users to use a version of the TikTok Global App in a country other than the United States version, if multiple versions exist, or to log into the TikTok Global App not as a TikTok U.S. User.

9.17 Monitoring of TikTok U.S. App and TikTok U.S. Platform Interactions and Systems for Non-U.S. TikTok Users.

(1) TTUSDS shall identify and monitor, and TTUSDS shall ensure the TTP identifies and monitors, for auditing purposes, all interactions and data elements exchanged between the TikTok U.S. App and TikTok U.S. Platform, on one hand, and systems operated by or on behalf of ByteDance serving non-U.S. TikTok Users, on the other hand. TTUSDS shall employ, and shall ensure that the TTP employs, technical means to block any such interactions that are unexpected or unauthorized, in the sole discretion of the TTP, and reports, within one (1) day of discovery and validation, any such interactions that have resulted or could reasonably result in unauthorized Access to, or other anomalous activity within, the TikTok U.S. App or the TikTok U.S. Platform to the Third-Party Monitor and the CMAs.

(2) TTUSDS shall ensure the TTP identifies and monitors for auditing purposes all interactions and data elements exchanged between the TikTok U.S. App and TikTok U.S. Platform, on one hand, and any Internet host and any other system or infrastructure, on the other hand. TTUSDS shall ensure the TTP employs technical means to block any such interactions that are unexpected or unauthorized, in the sole discretion of the TTP, and reports, within one (1) day of discovery and validation, any such interactions that have resulted or could reasonably result in unauthorized Access to, or other anomalous activity within, the TikTok U.S. App or TikTok U.S. Platform to the Third-Party Monitor and CMAs.

(3) The Transaction Parties shall ensure that encryption does not prevent the TTP from performing its obligations in connection with this Section 9.17.

(4) To the extent that the TTP's identification and monitoring activities under Sections 9.17(1)–(2) conflict with General Data Protection Regulation (“GDPR”) or other legal requirements, TTUSDS shall, within fourteen (14) days following the conflict arising: (i) provide written notice to the CMAs, including a detailed description of the legal requirements that create a conflict with citations to the relevant governing source(s); and (ii) coordinate with the TTP to present solutions to the CMAs that could be implemented to minimize the conflict to the greatest extent possible.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

9.18 Ongoing Risk Analysis. TTUSDS shall ensure the TTP assesses on an ongoing basis the risks posed to the national security of the United States and the privacy of TikTok U.S. Users, based on analysis of Source Code and Related Files, architectural analysis, and analysis of data flows, and that the TTP reports such findings to the Security Committee, Third-Party Monitor, and CMAs on a quarterly basis.

9.19 TTP Communications. ByteDance shall not inhibit, and shall ensure that none of its Affiliates inhibit, whether through the MSA or other means, TTUSDS's or the TTP's ability to communicate with each other, with the Third-Party Monitor, with the CMAs, or with any other appropriate USG authority, in each case independently and without the involvement or awareness of ByteDance or its Affiliates.

**ARTICLE X**

**TECHNOLOGY OFFICER**

10.1 Technology Officers. The Transaction Parties shall ensure the TTP appoints one (1) or more technology officers (the "**Technology Officers**") in each country where TTP Personnel are performing responsibilities in connection with the MSA to serve as the primary liaisons between the TTP and the Third-Party Monitor and CMAs and that the MSA fully incorporates the requirements of this Article X.

10.2 Qualifications of the Technology Officers. The Transaction Parties shall ensure that each Technology Officer:

- (1) is a Resident Sole U.S. Citizen who has, or is eligible for, a U.S. personnel security clearance for any Technology Officer in the United States, and if not in the United States, is a citizen of their country of residence;
- (2) has the appropriate senior-level authority and resources within the TTP and the necessary technical skills and experience to ensure compliance with this Agreement and to fulfill all other obligations of the position;
- (3) has no current or prior employment, contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates;
- (4) has Physical Access and Logical Access to all of the facilities, systems, records, and meetings of the TTP; and
- (5) regularly has Physical Access to the DTC necessary to ensure compliance with this Agreement.

The Transaction Parties shall ensure that if any Technology Officer holds other titles and responsibilities beyond serving as a Technology Officer for the purposes of this Agreement, such other responsibilities do not prevent the Technology Officer from performing his or her

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

obligations in connection with this Agreement and that the Technology Officer remains an employee of the TTP.

10.3 Initial Nomination of the Technology Officer.

(1) The appointment of each Technology Officer shall be subject to the prior non-objection of the CMAs. Within thirty (30) days following the Effective Date, the Transaction Parties shall ensure the TTP nominates each Technology Officer and submits complete Personal Identifier Information, a *curriculum vitae* or similar professional synopsis of the nominee, and any other information requested by the CMAs to assess whether the individual can effectively perform the obligations of the Technology Officer consistent with this Agreement. If the CMAs do not object within twenty-one (21) days following receipt of all necessary information about a nominee, the lack of action shall constitute a non-objection to that nominee. If the CMAs object, the Transaction Parties shall ensure the TTP nominates a different candidate within seven (7) days following receipt of any such objection, subject to the same procedures as the initial nomination. The Transaction Parties shall ensure the TTP appoints each Technology Officer within three (3) days following non-objection by the CMAs to that nominee.

10.4 Removal and Replacement.

(1) The Transaction Parties shall ensure the TTP does not remove any Technology Officer without the prior non-objection of the CMAs. The Transaction Parties shall ensure the TTP notifies the CMAs at least fourteen (14) days before the proposed removal of a Technology Officer unless such removal is for cause, and such a removal shall only be proposed in conjunction with the nomination of a new candidate for the position, to prevent a vacancy from taking place, subject to the same procedures as the initial nomination. Such cause must consist of willful misconduct, gross negligence, reckless disregard, violation of applicable law, violation of company policy, or failure of the individual to perform his or her job duties. The Transaction Parties shall ensure the TTP does not remove any Technology Officer for the Technology Officer's actual or attempted efforts to comply with or ensure compliance with this Agreement.

(2) Should the CMAs, in their sole discretion, determine that any Technology Officer has intentionally or through gross negligence failed to meet his or her obligations or has otherwise undermined the effectiveness of this Agreement, the CMAs may direct the TTP to remove such Technology Officer and the Transaction Parties shall ensure the TTP promptly, and in any event within two (2) days of such direction, removes such Technology Officer.

(3) In the event of any vacancy in any Technology Officer position, the Transaction Parties shall ensure the TTP notifies the CMAs within one (1) day and, within fourteen (14) days following such vacancy occurring, nominates a replacement Technology Officer, subject to the same process as the initial nomination.

10.5 Communication with the Third-Party Monitor and CMAs. The Transaction Parties shall ensure that each Technology Officer maintains reasonable availability for discussions with the Third-Party Monitor and CMAs on matters relating to compliance with this

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Agreement and has the ability to communicate with the Third-Party Monitor and CMAs independently and without the involvement or awareness of any of the Transaction Parties.

10.6 Reporting of Violations. The Transaction Parties shall ensure that each Technology Officer reports any actual or potential violation of this Agreement to the Security Officer, the Third-Party Monitor, and the CMAs as soon as practicable, but in any event within one (1) day of learning of the actual or potential violation.

10.7 Costs. The Transaction Parties shall be responsible for all costs associated with each Technology Officer.

**ARTICLE XI**

**PROTECTED DATA**

11.1 Excepted Data.

(1) Any proposed change to the categories of Excepted Data under Section 1.11, including Annexes A, B, and C, as applicable, shall be subject to the prior written consent of the CMAs. Prior to making any such change, the Transaction Parties shall submit a request to the CMAs identifying the additional data fields and formats proposed to become Excepted Data and shall include in the request the rationale for their designation as Excepted Data and any other information requested by the CMAs, in their sole discretion, to assess the request. The Transaction Parties shall not treat, and shall ensure the TTP does not treat, any Protected Data as Excepted Data without the prior written consent of the CMAs. If a change involves the categories outlined in Section 1.11(2) or (3), the Transaction Parties shall update Annexes A, B, and C, as applicable, and submit such updated Annexes to the Third-Party Monitor and CMAs within three (3) days following the Transaction Parties' receipt of the CMAs' consent.

(2) TTUSDS shall ensure that Excepted Data does not contain any Protected Data except in accordance with, as applicable, the fields and formats specified in Annexes A, B, and C before transmitting any Excepted Data to ByteDance, TikTok Inc., or their respective Affiliates, and shall make available, upon the request of the Third-Party Monitor or CMAs, evidence of compliance with this requirement. TTUSDS shall ensure that such evidence includes a review of logs from the gateways through which Excepted Data will transit, a review of system architecture to ensure those gateways are the sole transmission method for Excepted Data, and interviews with relevant TTUSDS and TTP Personnel. The Transaction Parties shall ensure that the Third-Party Monitor promptly, and in any event within one (1) day of discovery, reports to the CMAs any disclosure of Protected Data.

11.2 Public Data.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(1) The Transaction Parties shall not add new Public Data feature categories or implement any such changes in the TikTok U.S. App to collect additional Public Data feature categories, unless and until all of the following conditions are met:

(i) The Security Committee reviews and approves the designation of such feature categories as Public Data following a determination that public release of such feature categories is consistent with the privacy policy for the TikTok U.S. App (either existing or updated to address the release of such feature categories), the DPCP, and standard industry practice by U.S. social media companies, such as YouTube, Facebook, Instagram, and Twitter;

(ii) The Transaction Parties provide notice to the Third-Party Monitor and CMAs, including an updated version of Annex E, highlighting any new feature categories designated as Public Data with a rationale for each addition and screenshots of the TikTok U.S. App from the perspective of a TikTok U.S. User demonstrating that the data will be generally public unless an individual user makes such data private, in which case such data shall remain Protected Data for such individual;

(iii) TTUSDS provides notice using plain language to TikTok U.S. Users of any change to the privacy policy, if required, for the TikTok U.S. App, highlighting any new feature categories, and the rationale for making such change; and

(iv) The Transaction Parties have resolved any objections raised by the CMAs with the additional feature categories. If the CMAs do not raise any objections within sixty (60) days following receipt of notice under Section 11.2(1)(ii), the lack of action shall constitute a non-objection.

(2) The CMAs may raise objections to the collection of Public Data within approved feature categories or data fields within the feature categories by providing notice to the Security Committee. The Transaction Parties may explain why any such Public Data should remain public and the potential business and operational impact of changing it to Protected Data. If, after this process, the CMAs, in consultation with the Security Committee, determine that the relevant feature category or data field within a feature category should be re-designated as Protected Data, the Transaction Parties shall implement a plan to re-designate the applicable Public Data as Protected Data within ninety (90) days of receiving the request from the CMAs; *provided, however*, that such a re-designation shall not be required if the Security Committee confirms that such feature category or data field within a feature category is consistent, at the time of consideration, with the DPCP and standard industry practice by similar U.S. companies such as YouTube, Facebook, Instagram, and Twitter.

(3) TTUSDS shall not provide, and shall ensure the TTP does not provide, to ByteDance or any of its Affiliates any reports or datasets providing insights into Public Data to a greater extent than what a public Internet user could reasonably view or ascertain, without the prior review and approval by the Security Committee. For the avoidance of doubt, the limitations in this Section 11.2(3) shall not restrict ByteDance or any of its Affiliates from receiving: (i) videos at a higher resolution than is ultimately published on the TikTok U.S. App;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(ii) other Public Data and/or datasets related to Public Data where the Public Data elements are accessible to Internet users, but not ordinarily in volumes and at speeds needed to operate the TikTok global platform; and (iii) any reports that otherwise can be or are produced by third parties based on or derived from Public Data.

11.3 Expatriate TikTok U.S. User Requests.

(1) TTUSDS shall classify as a TikTok U.S. User any U.S. citizen who, upon registering through any version of the TikTok Global App, is not classified as a TikTok U.S. User and requests re-classification as a TikTok U.S. User, in accordance with a protocol to be developed by TTUSDS and subject to the prior non-objection of the CMAs (the “**Expatriate Request Protocol**”). At a minimum, TTUSDS shall ensure that such protocol provides for: (i) the option during new user registration on all versions of the TikTok Global App to allow U.S. citizens to select an option, and cause such user, to be re-classified as a TikTok U.S. User; (ii) sending a push notification to existing users of all versions of the TikTok Global App when first opened from a U.S. IP address notifying them of the option to be re-classified as a TikTok U.S. User if they are U.S. citizens; (iii) posting an article in the TikTok Global App Help Center regarding the option for U.S. citizens to be re-classified as a TikTok U.S. User; and (iv) including a feature within all versions of the TikTok Global App that enables users to select an option to be re-classified as a TikTok U.S. User if they are U.S. citizens. In order to minimize risks of conflicts of laws, TTUSDS may, subject to non-objection by the CMAs, implement a protocol that allows users outside the United States to present identification to a third party, who is not an Affiliate of ByteDance, that will confirm whether the user should be treated as a TikTok U.S. User. The Transaction Parties shall ensure that re-classification as a TikTok U.S. User is straightforward for users to find and complete.

(2) By no later than the Operational Date, the Transaction Parties shall submit the Expatriate Request Protocol to the Third-Party Monitor and CMAs. If the CMAs do not object in writing within fourteen (14) days following receipt of the Expatriate Request Protocol, the lack of action shall constitute a non-objection. If the CMAs object to the proposed Expatriate Request Protocol, the Transaction Parties shall address all concerns raised by the CMAs to the CMAs' satisfaction in a revised Expatriate Request Protocol submitted to the CMAs within fourteen (14) days following receipt of the written objection, which revisions shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial Expatriate Request Protocol. The Transaction Parties shall implement, and shall ensure the TTP implements, the Expatriate Request Protocol within three (3) days following the non-objection of the CMAs.

(3) To the extent that a request or class of requests by U.S. Citizens to re-classify as TikTok U.S. Users pursuant to Section 11.3(1) conflicts with GDPR or other legal requirements, TTUSDS shall: (i) provide written notice to the Security Committee and Third-Party Monitor, including a detailed description of the legal requirements that create a conflict with citations to the relevant governing source(s); and (ii) coordinate with the TTP to present solutions to the Security Committee and Third-Party Monitor that could be implemented to minimize the conflict to the greatest extent possible. TTUSDS shall ensure that the Security



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Committee consults quarterly with the CMAs regarding any such conflicts and works in good faith to address any concerns raised by the CMAs.

(4) TTUSDS shall ensure that the Security Committee reviews all requests by users of the TikTok U.S. App or other versions of the TikTok Global App to de-classify as TikTok U.S. Users, and only approves such requests, with the balance weighed in favor of denial, where: (i) the user has not within the past sixty (60) days accessed the TikTok U.S. App or any other versions of the TikTok Global App from within the United States; and (ii) the user identifies his or her appropriate country of citizenship.

11.4 End User Agreements and User Policies. TikTok Inc. and TTUSDS shall submit advance notice to the CMAs of any intention to change materially the Terms of Service, with such materiality to be determined in consultation with the Third-Party Monitor, the privacy policy for the TikTok U.S. App, content moderation policy, or other published policies similar thereto (each, a “**User Agreement**”) so the CMAs may review such User Agreements for consistency with this Agreement. Any material change, as determined in consultation with the Third-Party Monitor, to a User Agreement shall be subject to the prior non-objection of the CMAs except as otherwise provided herein. If the CMAs do not raise any objections within fifteen (15) days following receipt of the proposed change, the lack of action shall constitute a non-objection. TikTok Inc. and TTUSDS shall address all feedback from the CMAs prior to finalizing changes to any User Agreement; *provided, however*, that there shall be no limitation on finalizing such changes prior to the non-objection of the CMAs as long as TikTok Inc. and TTUSDS, as the case may be: (1) include in the original notice to the CMAs a clear explanation of the need for urgent implementation; and (2) address any feedback from the CMAs as promptly as possible after receipt. Notice to the CMAs pursuant to this Section 11.4 shall constitute notice only under this Section 11.4 and shall not satisfy any other notice requirements. Any feedback or non-objection by the CMAs under this Section 11.4 is specific to the change to the particular User Agreement and does not represent a USG determination applicable to any other context.

11.5 Protected Data Storage. The Transaction Parties shall ensure that all Protected Data, while such Protected Data remains in the possession of the Transaction Parties, is stored and remains: (1) exclusively in the United States, with no transmittal outside of the United States except as otherwise provided in this Agreement; and (2) within the TTP’s secure cloud environment, both except as expressly provided in this Agreement or otherwise by the prior written consent of the CMAs. The Transaction Parties shall ensure that any Protected Data transferred to third parties (and therefore not in the possession of the Transaction Parties) is subject to the vendor reviews and policies under Article XIII. For the avoidance of doubt, Section 11.5(1) shall not prohibit TTUSDS Personnel in DTC Approved Countries from Accessing Protected Data through the TTP’s secure cloud environment. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 11.5 to the Third-Party Monitor and CMAs.

11.6 User Interaction Data Deletion. The Transaction Parties shall ensure that all User Interaction Data in the possession of the Transaction Parties is deleted no later than eighteen (18) months after it is stored on the TikTok U.S. Platform or otherwise deleted in accordance with applicable law. For the avoidance of doubt, this deletion requirement applies to all data related

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

to individual users and their private interactions with content on the TikTok U.S. App (e.g., data on specific individuals who viewed or liked a video) but does not apply to aggregated data (e.g., the total number of views or likes a video has received).

11.7 Initial Transfer of Protected Data. By no later than the Operational Date, ByteDance shall transfer, and shall ensure that its Affiliates transfer, all Protected Data held by ByteDance and its Affiliates as of the Effective Date or acquired thereafter (collectively, the “**Legacy Protected Data**”) to the TTP (the date of such transfer, the “**Transfer Date**”); *provided, however,* that if any Legacy Protected Data is subject to any litigation hold or legal preservation requirement as of the Transfer Date, ByteDance may transfer such Protected Data to a third-party approved in advance by the CMAs to hold such data in escrow pending satisfaction of the applicable litigation hold or legal preservation requirement. On or prior to the Transfer Date, ByteDance shall notify the CMAs in writing of any litigation hold or legal preservation requirement applicable to any Legacy Protected Data. ByteDance shall provide written confirmation to the Third-Party Monitor and CMAs promptly upon the successful transfer of all Legacy Protected Data, or report ByteDance’s failure to transfer all Legacy Protected Data by the Transfer Date.

(1) Within one-hundred twenty (120) days following confirmation that all Legacy Protected Data has been successfully transferred (the “**Deletion Date**”), ByteDance shall irretrievably destroy, or cause to be irretrievably destroyed, all Protected Data, including copies thereof, wherever located, in the possession or control of ByteDance or any of its Affiliates, in accordance with the “Clear” level articulated in the NIST principles for sanitization and destruction of data. ByteDance shall submit monthly reports to the Third-Party Monitor and CMAs on its progress destroying Protected Data by the deadline herein.

(2) Within sixty (60) days following the Deletion Date, the Transaction Parties shall ensure that all assets and operations in the United States of the Transaction Parties and their respective Affiliates that support, or have supported, the TikTok U.S. App and TikTok U.S. Platform undergo one or more audits (each, a “**U.S. Deletion Audit**”) to confirm the irretrievable destruction of all Protected Data. The auditor, timing, scope, and methodology of the U.S. Deletion Audits shall be subject to the prior non-objection of the CMAs. By no later than the Deletion Date, the Transaction Parties shall submit sufficient information regarding the proposed auditor and scope of the U.S. Deletion Audits for the CMAs to assess the nominee and proposal. If the CMAs do not object in writing to the nominee and proposal within twenty-one (21) days following receipt, the lack of action shall constitute a non-objection. The Transaction Parties shall ensure that the auditor starts the initial U.S. Deletion Audit within five (5) days following the CMAs’ non-objection and completes the initial U.S. Deletion Audit consistent with the proposal. If the CMAs object to the proposed auditor or proposal, the Transaction Parties shall submit an alternative auditor or modified proposal, as applicable, which resolves the concerns raised to the CMAs’ satisfaction, within fourteen (14) days following the Transaction Party’s receipt of any such objection, subject to the same procedures as the initial review. The Transaction Parties shall ensure that the auditor provides the results of each U.S. Deletion Audit to the CMAs within three (3) days following its completion. The Transaction Parties shall take, and shall ensure that their respective Affiliates take, all remedial actions deemed necessary by

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

the auditor or CMAs, in their sole discretion, based upon the results of any U.S. Deletion Audit within thirty (30) days of its completion unless otherwise extended in writing by the CMAs (including shutting down IT systems that continue to store or provide Access to Protected Data until such time that all Protected Data is irretrievably destroyed). The Transaction Parties shall provide, and shall ensure that their respective Affiliates provide, the auditor with all Physical Access and Logical Access necessary to interview Personnel and to conduct the U.S. Deletion Audits within the scope approved by the CMAs, including Physical Access and Logical Access to inspect any IT systems, networks, hardware and software, data, communications systems, properties, records and documents, and correspondence in the possession or control of the Transaction Parties. The Transaction Parties shall be responsible for all costs and expenses in connection with the U.S. Deletion Audits.

(3) Within sixty (60) days following the Deletion Date, ByteDance shall further certify, through verification processes developed in coordination with a third party retained by and at the sole expense of ByteDance and subject to the CMAs' approval, that all Protected Data has been irretrievably destroyed globally (the "**Global Deletion Verification**"). ByteDance shall take, and shall ensure that its Affiliates take, all remedial actions identified by the third party, in its sole discretion, as a result of the Global Deletion Verification within thirty (30) days of its completion unless otherwise extended in writing by the CMAs (including shutting down IT systems that continue to store or provide Access to Protected Data until such time that all Protected Data is irretrievably destroyed). ByteDance shall provide, and shall ensure that its Affiliates provide, the third party with all Physical Access and Logical Access necessary to conduct the Global Deletion Verification, including Physical Access and Logical Access to interview Personnel and to inspect any IT systems, networks, hardware and software, data, communications systems, properties, records and documents, and correspondence in the possession or control of the Transaction Parties. ByteDance shall deliver the certification of the Global Deletion Verification to the CMAs no later than fourteen (14) days following completion of the Global Deletion Verification. Thereafter, ByteDance shall annually certify, on behalf of itself and its Affiliates, to the CMAs that it does not possess, and cannot Access, any Protected Data or copies thereof.

11.8 Restricted Access to Protected Data. Following the Deletion Date, ByteDance and TikTok Inc. shall not take possession of or Access, and shall ensure that none of their respective Affiliates take possession of or Access, any Protected Data, whether Legacy Protected Data or Protected Data collected, derived, or stored on or after the Transfer Date, without the prior written consent of the CMAs. For the avoidance of doubt, this Section 11.8 shall not limit ByteDance's Access to Excepted Data or Public Data in accordance with this Agreement. TTUSDS shall ensure that Access to Protected Data is limited to those Personnel who require Access to fulfill their assigned job responsibilities. The Transaction Parties shall ensure the TTP implements controls and safeguards to ensure compliance with these requirements, including: (1) Physical and Logical Access controls necessary to safeguard Protected Data generally; and (2) the ability to refuse Logical Access by the Transaction Parties or any Affiliate thereof to Protected Data. In the event that a TTP is removed or replaced, TTUSDS shall ensure the previous TTP retains control of all Protected Data unless and until the CMAs consent to a new TTP or an alternate custodian of Protected Data. The Transaction Parties shall ensure the TTP

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

promptly reports any non-compliance with this Section 11.8 to the Third-Party Monitor and CMAs.

11.9 Limited Access to Protected Data. Notwithstanding the restrictions in Sections 11.8 and 11.10, in addition to TTUSDS Personnel who require Access to Protected Data to fulfill their assigned job responsibilities, certain Personnel of the Transaction Parties and their Affiliates may Access certain fields of Protected Data for the limited purposes of addressing legal and compliance matters and certain other emergency situations involving the health, safety, and security of TikTok users and the public in and outside the United States; *provided* that any such Access is strictly in accordance with a protocol (the “**Limited Access Protocol**”) developed by the Transaction Parties and the TTP and subject to the prior non-objection of the CMAs.

(1) In the Limited Access Protocol, the Transaction Parties shall, among other issues, identify all circumstances under which certain ByteDance or TikTok Inc. Personnel may Access Protected Data; the requirements related to those Personnel, including any citizenship, residency, location, and screening requirements; the particular fields and formats of the Protected Data such Personnel may Access; and the method for providing such Access to Protected Data, which shall be through a secure, auditable environment created and maintained by the TTP.

(2) Prior to ByteDance, TikTok Inc., or any of their respective Affiliates having any Access to Protected Data under this Section 11.9, the Transaction Parties shall submit the Limited Access Protocols to the Third-Party Monitor and CMAs. If the CMAs do not object in writing within thirty (30) days following receipt of the Limited Access Protocol, the lack of action shall constitute a non-objection. If the CMAs object to the proposed Limited Access Protocol, the Transaction Parties shall address all concerns raised by the CMAs to the CMAs' satisfaction in a revised Limited Access Protocol submitted to the CMAs within thirty (30) days following receipt of the written objection, which shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial Limited Access Protocol. The Transaction Parties shall fully implement, and shall ensure the TTP fully implements, the Limited Access Protocol prior to ByteDance, TikTok Inc., or any of their respective Affiliates having any Access to Protected Data under this Section 11.9. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with the Limited Access Protocol or this Section 11.9 to the Third-Party Monitor and CMAs.

11.10 Restricted Persons. The Transaction Parties shall not transfer, and shall ensure that none of their respective Affiliates or the TTP transfer, any Protected Data to any CFIUS Restricted Persons unless otherwise approved by the CMAs. The Transaction Parties shall ensure that any Protected Data transferred to third parties (and therefore not in the possession of the Transaction Parties) is subject to the vendor reviews and policies under Article XIII. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 11.10 to the Third-Party Monitor and CMAs.

11.11 Separate Credentials. By no later than the Operational Date, TTUSDS shall ensure the TTP implements controls such that any Logical Access to Protected Data requires additional, separate credentials. TTUSDS shall ensure that the controls implemented jointly by the TTP via the MSA and TTUSDS require credentials that are based on security best practices

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(e.g., multiple factors of authentication) and restrict Logical Access based on a Person's physical location to the fullest extent possible and need to Access Protected Data to fulfill his or her assigned job responsibilities, in order to ensure compliance with this Agreement. TTUSDS shall ensure the TTP only allows Personnel of the TTP and TTUSDS who need Access to fulfill their assigned job responsibilities, or other Persons only in accordance with the Limited Access Protocol or with prior written consent of the CMAs, to hold credentials that allow Logical Access to Protected Data.

11.12 Data Security Certifications. Each of the Transaction Parties shall submit, and shall ensure the TTP submits, to the CMAs, on a semiannual basis, a certification regarding its full compliance with this Agreement's requirements related to Protected Data.

11.13 Training by the TTP. TTUSDS shall ensure the TTP regularly, and not less than annually, trains the TTP's relevant Personnel (including training new relevant Personnel as part of the initial onboarding process) on the MSA and this Agreement's requirements related to Protected Data.

## ARTICLE XII

### DATA PRIVACY AND CYBERSECURITY PROGRAM

12.1 Program Establishment. TTUSDS shall establish and maintain, and shall ensure the TTP establishes and maintains, a comprehensive data privacy and cybersecurity program (each, a "DPCP") that shall include policies and procedures to ensure compliance with this Agreement, including measures to safeguard Protected Data, Excepted Data, and Public Data (each as within the respective possession of TTUSDS and the TTP) and to enforce the Physical Access and Logical Access restrictions and Source Code and Related Files security measures. For the avoidance of doubt, the TTP DPCP shall only apply with respect to the TTP's roles and responsibilities as defined by the MSA.

(1) TTUSDS, in coordination with the TTP and Third-Party Monitor, shall develop the DPCP in accordance with standards developed or published by the following standards organizations and/or as further specified: (i) NIST, including NIST Special Publication 800-82, Guide to Industrial Control Systems (2015); (ii) the NIST Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1 (January 10, 2017); (iii) NIST Special Publications 800-53 and 800-171, Revision 4; (iv) ISO, including ISO/IEC 27001 and 27002 standards; (v) the successor versions of each of Section 12.1(1)(i)-(iv); (v) the Center for Internet Security; or (vi) another standards organization with provisions pertaining to data protection as communicated by the Third-Party Monitor or CMAs.

(2) TTUSDS, in coordination with the TTP and Third-Party Monitor, shall ensure that the DPCP includes, consistent with the framework on which it is based, provisions for: the encryption of all Protected Data, Excepted Data, and Public Data in transit and select Protected Data, Excepted Data, and Public Data at rest as identified in the DPCP; inventory of authorized devices, software, hardware, applications, and credentials; secure configurations of systems and devices; data recovery; security training; Physical Access and Logical Access

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

controls; log controls; incident detection, handling, and response; penetration testing; and other robust processes and protections necessary for the activities set forth in this Agreement, including the secure submission and inspection of Source Code and Related Files, persistent monitoring of interactions of the TikTok U.S. App and TikTok U.S. Platform, unauthorized Access to or transmission of Protected Data, and other requirements set forth under this Agreement.

(3) TTUSDS, in coordination with the Third-Party Monitor, shall ensure that the DPCP provides for independent IT systems, networks, communications systems, and other resources that are logically segregated from those of ByteDance or any of its Affiliates, and to which none of ByteDance or any of its Affiliates has any Access.

(4) TTUSDS, in coordination with the TTP and Third-Party Monitor, shall ensure that the DPCP provides for an annual vulnerability assessment of the TikTok U.S. App and TikTok U.S. Platform to be conducted by the TTP. TTUSDS shall ensure that the Security Officer and Technology Officer jointly report the findings of such vulnerability assessments to the Third-Party Monitor and CMAs, along with their plans to address any such findings.

(5) As part of the DPCP, TTUSDS shall develop, and shall ensure the TTP implements, a violation reporting plan requiring all Personnel to report actual or potential violations of this Agreement or the DPCP to the Security Officer (in the case of TTUSDS) or Technology Officer (in the case of the TTP). Such plan shall include protections against retaliation for all Personnel.

12.2 Adoption. The adoption of the DPCP shall be subject to the prior non-objection of the CMAs. TTUSDS, in coordination with the TTP and Third-Party Monitor, shall submit a draft of the DPCP to the CMAs within thirty (30) days following the Operational Date. If the CMAs do not object in writing to the draft DPCP within thirty (30) days following receipt, the lack of action shall constitute a non-objection. If the CMAs object to the proposed DPCP, TTUSDS shall address, and shall ensure the TTP addresses, all concerns raised by the CMAs to the CMAs' satisfaction in a revised draft of the DPCP submitted to the CMAs within thirty (30) days following receipt of the written objection, which revised draft shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial draft. TTUSDS shall implement, and shall ensure the TTP implements, the DPCP within three (3) days following non-objection of the CMAs.

12.3 Amendment. If at any time TTUSDS (including the Security Committee), the TTP, or the CMAs determine that the DPCP should be amended, TTUSDS shall engage, in coordination with the TTP and Third-Party Monitor, with the CMAs to amend the DPCP. Any amendment of the DPCP shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial draft of the DPCP.

12.4 Dissemination and Training. Within thirty (30) days following the non-objection of the CMAs to the DPCP, TTUSDS shall disseminate, and shall ensure the TTP disseminates, the DPCP to all appropriate Personnel. TTUSDS, in coordination with the TTP, shall ensure that all appropriate existing and new Personnel of TTUSDS and the TTP receive training on the

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

DPCP (the “**Training**”). TTUSDS shall ensure that all appropriate new Personnel of TTUSDS and the TTP receive the DPCP and complete the Training, and that all such existing Personnel complete a refresher Training at least annually. TTUSDS shall ensure that the Security Officer (in the case of TTUSDS) and the Technology Officer (in the case of the TTP) implement and oversee the dissemination and Training processes.

12.5 Confidentiality. TTUSDS shall not share, and shall ensure the TTP does not share, the DPCP or any contents thereof with ByteDance or any of its Affiliates, including their respective Personnel, without the prior written consent of the CMAs.

12.6 Violations. TTUSDS shall ensure that the Security Officer and Technology Officer report any actual or potential violation of the DPCP and any remedial actions taken to the CMAs as soon as practicable, and in any event within one (1) day of discovery of the actual or potential violation. TTUSDS shall ensure that the Security Officer and Technology Officer each independently maintain a log of any reports received from individuals regarding perceived violations of the DPCP, whether or not ultimately reported to the CMAs. Any violation of the DPCP shall be deemed to constitute a violation of this Agreement, and the failure by TTUSDS or the TTP to obtain authorizations and approvals that are necessary to comply with the DPCP shall not excuse a violation of the DPCP.

**ARTICLE XIII**

**VENDOR APPROVALS**

13.1 Identification of Vendors. Within ninety (90) days following the Effective Date, the Transaction Parties shall submit to the Security Committee, Third-Party Monitor, and CMAs (or, if the Third-Party Monitor has not been engaged by the time of submission, within three (3) days following its engagement):

(1) a list and description of all third-party contracts and other arrangements as of the Effective Date with third parties that support or will support the TikTok U.S. App or the TikTok U.S. Platform, or that otherwise support TTUSDS and have Access to Protected Data or systems on which Protected Data is stored, or that otherwise provide for the sale of Protected Data, other than those on the Existing Vendors and Contracts List (as defined below).

(2) a list and description of contracts that are with the TTP or vendors directly contracted by the TTP as of the Effective Date (the lists and summaries identified in clauses (1) and (2) of this Section 13.1 collectively, the “**Existing Vendors and Contracts List**”).

The Transaction Parties shall ensure that the Existing Vendors and Contracts List identifies the following information for each contract: the vendor (including its place of legal organization and principal place of business), the service provided, and any equipment supplied.

13.2 Thereafter, TTUSDS shall, periodically and no less frequently than semi-annually, review the same information described in Section 13.1(1) for each such contract, vendor, and other arrangement that is in place, update it as necessary to be accurate and complete

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

as of the date of review, and submit the updated information to the Third-Party Monitor (each such list, a “**Vendors and Contracts List**”). The Transaction Parties shall ensure that the Third-Party Monitor reviews the Existing Vendors and Contracts List used by TTUSDS and each Vendors and Contracts List and identifies all contracts that could permit a vendor to Access Protected Data or the TikTok U.S. Platform through TTUSDS (collectively, the “**Existing Vendor Contracts**”) and notifies the Security Committee and the CMAs of all Existing Vendor Contracts. TTUSDS shall ensure that the Security Committee and Third-Party Monitor provide to the CMAs, within seven (7) days of a request by the CMAs, information regarding any current or prospective third-party vendors, contracts with third-party vendors, or information regarding the review of any current or prospective third-party vendor.

13.3 Review of Existing Vendor Contracts. TTUSDS shall ensure that, within forty-five (45) days following any submission under Section 13.1, the Security Committee evaluates all of the Existing Vendor Contracts, with review and oversight by the Third-Party Monitor, to determine if they are consistent with the obligations under this Agreement, and identify, in the Security Committee’s sole discretion, any Existing Vendor Contracts that may allow for actions contrary to this Agreement and any information regarding any vendor party to any Existing Vendor Contract that causes the Security Committee to believe that the vendor’s engagement under such Existing Vendor Contract has undermined, or would be reasonably likely to undermine, the effectiveness of this Agreement, including, as appropriate, the vendor’s ability to meet its obligations under such Existing Vendor Contract. In evaluating any Existing Vendor Contract, TTUSDS shall ensure that the Security Committee and Third-Party Monitor consider any concerns identified by the CMAs. TTUSDS shall ensure that, upon a conclusion by the Security Committee and Third-Party Monitor, or, in the event that the Security Committee and the Third-Party Monitor do not reach consensus, by the CMAs, that any Existing Vendor Contract undermines or is contrary to this Agreement or that information regarding any vendor party to an Existing Vendor Contract supports a concern that engagement of the vendor under an Existing Vendor Contract has undermined, or is reasonably likely to undermine, the effectiveness of this Agreement, including, as appropriate, a concern that the vendor is unable to meet its obligations under an Existing Vendor Contract (each such determination, a “**Contrary Determination**”), the Security Committee and/or the Third-Party Monitor shall notify TTUSDS to which the Existing Vendor Contract relates, and TTUSDS shall immediately: (1) cause the termination or modification of such Existing Vendor Contract so that it no longer allows for actions contrary to this Agreement, as determined by the Security Committee and/or Third-Party Monitor in their sole discretion; (2) cause the termination of any role by a vendor party to such Existing Vendor Contract so that it is no longer a party to the Existing Vendor Contract; (3) take all actions necessary to end and prevent Logical Access to Protected Data or the TikTok U.S. Platform by the vendor at issue until a revised contract is executed or a new vendor is substituted, if applicable, that resolves the concerns of the Security Committee and Third-Party Monitor, in their sole discretion, and if applicable; and (4) notify the CMAs within three (3) days of the Contrary Determination.

(1) Within fourteen (14) days following the later of the completion by the Security Committee and Third-Party Monitor of a review of Existing Vendor Contracts and by TTUSDS of action regarding any Contrary Determination, TTUSDS shall notify the Third-Party



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Monitor and the CMAs of: (i) any Existing Vendor Contracts that have been terminated or modified; (ii) any vendors terminated as a party to an Existing Vendor Contract; (iii) the reason for such termination or modification; and (iv) all other actions taken to address a Contrary Determination.

13.4 New Vendor Contracts. TTUSDS shall not enter into, and shall ensure that its Affiliates do not enter into, any contract with a vendor that undermines or is contrary to this Agreement. TTUSDS, with the oversight of the Third-Party Monitor, shall ensure that the Security Committee continues to review all potential (other than routine commercial transactions between TTUSDS and advertising or e-commerce customers) contracts with new vendors or existing vendors providing a new type of service, in each case that will support the TikTok U.S. App, the TikTok U.S. Platform, or that otherwise support TTUSDS and have Access to Protected Data or systems on which Protected Data is stored (any such contract, a “**New Vendor Contract**”). TTUSDS shall ensure that the Security Committee notifies the Security Officer, Third-Party Monitor, and CMAs of any New Vendor Contracts that undermine or are contrary to this Agreement, including based on information regarding any vendor party to a New Vendor Contract that supports a concern that engagement of the vendor under a New Vendor Contract has undermined, or is reasonably likely to undermine, the effectiveness of this Agreement, including, as appropriate, a concern that the vendor will be unable to meet its obligations under a New Vendor Contract. Where the Security Committee determines that a potential New Vendor Contract is not consistent with this Agreement in its sole discretion, the Transaction Parties shall not execute such contract. Upon request by the CMAs, TTUSDS shall provide the CMAs with a list of New Vendor Contracts.

13.5 Vendor Program Policy. TTUSDS, in coordination with the Third-Party Monitor, shall implement a program (the “**Vendor Program**”) whereby all New Vendor Contracts (including, for the avoidance of doubt, the vendors who are parties to such contracts) will be subject to initial and periodic review and non-objection by the Third-Party Monitor against criteria and risk factors to be identified, and TTUSDS shall adopt a written policy for the Vendor Program (the “**Vendor Program Policy**”), subject to the prior review and non-objection of the Security Committee and the CMAs. The Transaction Parties shall comply with the requirements of the Vendor Program Policy and shall share all necessary information with TTUSDS and the Third-Party Monitor to implement the Vendor Program Policy.

(1) TTUSDS shall submit a draft Vendor Program Policy to the Third-Party Monitor and CMAs by no later than ninety (90) days following the Operational Date.

(2) The adoption of the Vendor Program Policy shall be subject to the prior non-objection of the CMAs. If the CMAs do not object in writing to the draft Vendor Program Policy within thirty (30) days following receipt, the lack of action shall constitute a non-objection. If the CMAs object to the draft Vendor Program Policy, TTUSDS shall address all concerns raised to the CMAs' satisfaction and submit a revised draft of the Vendor Program Policy to the CMAs within twenty-one (21) days following receipt of the written objection, which subsequent draft shall be subject to the same procedures as the initial draft. TTUSDS shall adopt the Vendor Program Policy within three (3) days following the non-objection of the CMAs. Upon adoption of the Vendor Program Policy, the Transaction Parties shall not execute,

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

finalize, or implement any New Vendor Contract that is inconsistent with the Vendor Program Policy, including the requirement to obtain the prior non-objection of the Third-Party Monitor. Any revisions or amendments to the Vendor Program Policy shall be subject to the prior non-objection of the CMAs, subject to the same procedures as the initial draft.

(3) TTUSDS shall ensure that the Security Committee, with oversight by the Third-Party Monitor, oversees and maintains the Vendor Program Policy governing New Vendor Contracts to ensure compliance with this Agreement and the Vendor Program Policy. TTUSDS shall ensure that the Security Committee and the Third-Party Monitor have the authority to approve, reject, mitigate, or otherwise condition the engagement of any New Vendor Contract or any vendor party to a New Vendor Contract. TTUSDS shall ensure that any New Vendor Contract: (i) explicitly incorporates the requirements of this Agreement, as applicable, and (ii) provides TTUSDS with any contractual rights it will require to comply with the Vendor Program Policy, including to assess the risk factors set forth in the Vendor Program Policy and to periodically review third-party vendors.

(4) TTUSDS shall ensure that the Security Committee and Third-Party Monitor considers any information provided by the CMAs regarding current or prospective New Vendor Contracts or vendors party to New Vendor Contracts and implements any recommendations from the CMAs regarding approving, rejecting, mitigating, or otherwise conditioning the engagement of any New Vendor Contract or any vendor party to a New Vendor Contract. To support any such recommendation, the CMAs may provide a justification to the Security Committee and Third-Party Monitor, based on relevant available unclassified information. To the extent that the recommendation is predicated on classified information, or other information that cannot be shared with the Security Committee and Third-Party Monitor, the CMAs may indicate so and share the relevant information with those Security Committee members, if any, who do possess the requisite qualifications for Access to such information.

(5) TTUSDS shall ensure that the Vendor Policy Program, at a minimum, evaluates third-party vendors based on risk factors including: (a) the type, functionality and intended location of equipment, products, or services to be provided by the third-party vendor; (b) the intended usage and deployment of such equipment, products, or services to or within a DTC and the TikTok U.S. Platform; (c) the nature of Access to Protected Data, Source Code and Related Files, the TikTok U.S. Platform, or other sensitive operations of TTUSDS or the TTP to be granted to the third-party vendor; (d) the third-party vendor's record of compliance with relevant U.S. laws, regulations, standards, and contracts, as well as any applicable domestic or international data protection laws and regulations; (e) the third-party vendor's record of compliance with cybersecurity standards and any security breaches, to the extent known; (f) the country in which the third-party vendor maintains its principal place of business or conducts substantial operations; and (vi) any other risk factors identified by the Third-Party Monitor or CMAs in their sole discretion.

13.6 CMA Waivers. In connection with the review of the Existing Vendors and Contracts List, each Vendors and Contracts List, New Vendor Contracts, and the development and implementation of a Vendor Program Policy, TTUSDS may request, and the CMAs may

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

grant in their sole discretion, a waiver for any individual third-party vendors to be exempt for a specified period of time or completely from such future reviews.

13.7 TTP Access to Vendor Information. TTUSDS shall ensure the TTP has Access to all vendor information it needs to discharge its responsibilities under this Agreement. For the avoidance of doubt, there is a presumption that the sharing of commercially sensitive competitive pricing or related information shall not be necessary for the TTP to discharge its responsibilities under this Agreement.

**ARTICLE XIV**

**CYBERSECURITY AUDITS**

14.1 Cybersecurity Audit. TTUSDS shall engage, at its own expense, a U.S.-based independent third party that has no current or prior contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates, unless otherwise agreed to by the CMAs (the “**Cybersecurity Auditor**”), to conduct and complete a cybersecurity audit and prepare a report regarding its findings (the “**Cybersecurity Audit**”). TTUSDS shall, in coordination with the TTP, propose the terms, scope, methodology, and timeframe for completion of the Cybersecurity Audit (the “**Cybersecurity Audit Plan**”). The Cybersecurity Auditor and Cybersecurity Audit Plan shall be subject to the prior non-objection of the CMAs. TTUSDS shall ensure that the Cybersecurity Audit is undertaken in accordance with the Cybersecurity Audit Plan and includes an audit of each of the following:

- (1) the TTP’s deployment of the TikTok U.S. Platform;
- (2) the establishment of the DTC and implementation of the DTC Operating Protocols;
- (3) TTUSDS’s and the TTP’s processes and tools for reviewing, inspecting, and compiling Source Code and Related Files and deployment of Executable Code in accordance with Section 9.10;
- (4) the identification of any vulnerabilities designated as high severity or equivalent, including any instance of Malicious Code in the Source Code and Related Files or Executable Code, and the remediation of such issues;
- (5) the implementation and effectiveness of the mobile sandbox for the TikTok U.S. App pursuant to Section 9.8;
- (6) the storage and protection of Protected Data, including verification of the newly created credentials for Logical Access to Protected Data and that none of the Transaction Parties has Access to Protected Data except as permitted under this Agreement;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(7) the secure and fully auditable environment through which Personnel of the ByteDance and its Affiliates may Access certain fields of Protected Data pursuant to the Limited Access Protocol; and

(8) TTUSDS's and the TTP's implementation of and compliance with the DPCP.

14.2 Cybersecurity Auditor and Audit Plan.

(1) Within one hundred and eighty (180) days following the Operational Date, TTUSDS shall submit to the CMAs the name of the proposed Cybersecurity Auditor, the proposed terms of engagement, and any other information requested by the CMAs to assess the proposal. If the CMAs do not object in writing within thirty (30) days following receipt of all necessary information, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to the proposed Cybersecurity Auditor or terms of engagement, TTUSDS shall, within fourteen (14) days following receipt of any such objection, propose a different Cybersecurity Auditor and make changes to the proposed terms of engagement, in each case subject to the same procedures as the initial proposal. If the CMAs object to the second proposed Cybersecurity Auditor, TTUSDS shall, within fourteen (14) days following receipt of such objection, propose three (3) Cybersecurity Auditors, from which the CMAs may select the Cybersecurity Auditor. TTUSDS shall engage the Cybersecurity Auditor within three (3) days following the non-objection of, or (if applicable) selection by, the CMAs.

(2) TTUSDS, in coordination with the TTP and Third-Party Monitor, shall develop the Cybersecurity Audit Plan and, no later than twenty-one (21) days following the engagement of the Cybersecurity Auditor, submit the proposed Cybersecurity Audit Plan to the CMAs. If the CMAs do not object in writing within twenty-one (21) days following receipt of the Cybersecurity Audit Plan, the lack of action shall constitute a non-objection. If the CMAs object, TTUSDS shall, in coordination with the TTP and Third-Party Monitor and within fourteen (14) days following receipt of such objection, resolve all concerns raised by the CMAs and submit a revised Cybersecurity Audit Plan to the CMAs, subject to the same procedures as the initial proposal. TTUSDS shall ensure that the Cybersecurity Auditor fully completes the Cybersecurity Audit in accordance with the Cybersecurity Audit Plan.

14.3 Review of Findings. TTUSDS shall ensure that the Security Officer and Technology Officer, in consultation with the Security Committee, have the opportunity to review and comment on the preliminary findings of the Cybersecurity Audit. TTUSDS shall ensure that the Cybersecurity Auditor submits to the CMAs the preliminary and final Cybersecurity Audit report findings within three (3) days of the completion of each such report, and that the Security Officer and Technology Officer submit to the CMAs their responses to such reports.

14.4 Implementation Plan. Following completion of the Cybersecurity Audit and submission of the final Cybersecurity Audit report, TTUSDS shall ensure that the Security Officer submits to the CMAs a plan for implementing all recommendations arising from the Cybersecurity Audit within sixty (60) days following receipt of the final Cybersecurity Audit report. TTUSDS shall fully implement such plan within sixty (60) days following its submission

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

of its remediation plan to the CMAs, absent an objection by the CMAs to such plan or CMA approval for another timeline. If the CMAs object to the plan, TTUSDS shall resolve any concerns raised by the CMAs, including by submitting a revised implementation plan for CMA review if requested by the CMAs, within such reasonable period of time as determined by the CMAs in their sole discretion.

14.5 Additional Cybersecurity Audits. The CMAs may, in their sole discretion, require TTUSDS to undertake additional Cybersecurity Audits, subject to the same procedures as the initial Cybersecurity Audit, but no more than once (1) per year.

14.6 Costs of the Cybersecurity Audits. TTUSDS shall be responsible for all fees, costs, and expenses related to any Cybersecurity Audit.

## ARTICLE XV

### THIRD-PARTY AUDITS

15.1 Upon a request by the CMAs, but no more than once (1) per year, each Transaction Party shall, at its own expense, engage a U.S.-based third-party independent auditor (the “**Third-Party Auditor**”) to assess its overall compliance with this Agreement (the “**Audit**”). For the avoidance of doubt, the Transaction Parties may propose the same third-party independent auditor. The relevant Transaction Party shall ensure that the Third-Party Auditor is available to meet and confer with the CMAs independent of any of the other Transaction Parties.

(1) Review by CMAs. The Third-Party Auditor and the scope, methodology, and timeframe for completion of the Audit (the “**Audit Plan**”) shall be subject to prior non-objection of the CMAs. The relevant Transaction Party shall submit sufficient information for the proposed Third-Party Auditor and Audit Plan for the CMAs to assess the nominee and proposal within thirty (30) days following the request of the CMAs. If the CMAs do not object in writing to the Third-Party Auditor and the Audit Plan within thirty (30) days following receipt, the lack of action shall constitute a non-objection. The relevant Transaction Party shall ensure that the Third-Party Auditor starts the Audit within five (5) days following the CMAs’ non-objection and fully completes the Audit in accordance with the Audit Plan. If the CMAs object to the proposed Third-Party Auditor or Audit Plan, the Transaction Party shall submit an alternative Third-Party Auditor or modified Audit Plan, which in each case shall resolve the concerns raised to the CMAs’ satisfaction, within fifteen (15) days following the Transaction Party’s receipt of any such objection, subject to the same procedures as the initial nominee or proposal, as applicable. The Transaction Parties shall be responsible for all fees, costs, and expenses related to any Audits.

(2) Audit Report. Each Transaction Party shall require the respective Third-Party Auditor to produce a written final Audit report, which shall include a list of any identified vulnerabilities or deficiencies that have affected or could affect such Transaction Party’s compliance with this Agreement. The Transaction Party shall ensure that the audit report is provided to the Security Committee, the Security Officer, the Third-Party Monitor, and the

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

CMAs. The CMAs may require supplemental reports if any final audit report is not consistent with the CMAs' expectations related to the details of the analysis and conclusions presented.

**ARTICLE XVI**

**THIRD-PARTY MONITOR**

16.1 **Engagement.** Within thirty (30) days following the Effective Date, the Transaction Parties shall nominate an independent third-party monitor (the "**Third-Party Monitor**") to monitor the Transaction Parties' compliance with this Agreement and serve as a point of contact for the CMAs. The engagement of the Third-Party Monitor shall be subject to the prior non-objection of the CMAs. The Transaction Parties shall submit sufficient information to allow the CMAs to assess the nominee. If the CMAs do not object in writing within thirty (30) days following receipt of all information necessary to assess the nominee, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to the proposed nominee, the Transaction Parties shall nominate a different candidate within five (5) days following receipt of any such objection, subject to the same procedures as the initial nomination. If the CMAs object to the second proposed Third-Party Monitor, within fourteen (14) days following receipt of such objection, the Transaction Parties shall propose three (3) candidates meeting the qualifications set forth in Section 16.2, from which the CMAs may select the Third-Party Monitor. TTUSDS shall engage the Third-Party Monitor within three (3) days following the non-objection of, or (if applicable) selection by, the CMAs. TTUSDS shall not remove or replace the Third-Party Monitor without the prior written consent of the CMAs, and TTUSDS shall nominate a replacement Third-Party Monitor within five (5) days following such removal, subject to the same procedures as the initial nomination. The CMAs, in their sole discretion, may direct TTUSDS to terminate the Third-Party Monitor and TTUSDS shall promptly, and in any event within three (3) days of such direction, terminate the Third-Party Monitor. In the event that there is a vacancy in the Third-Party Monitor position due to removal by the CMAs, resignation by the Third-Party Monitor, or otherwise, TTUSDS shall nominate a replacement Third-Party Monitor within twenty-one (21) days following such vacancy, subject to the same procedures as the initial nomination.

16.2 **Qualifications.** The Transaction Parties shall ensure that the Third-Party Monitor is an entity incorporated and with its principal place of business in the United States and uses only Resident U.S. Citizens to monitor compliance with this Agreement, in each case unless otherwise approved by the CMAs. The Transaction Parties shall ensure that the Third-Party Monitor possesses qualifications appropriate for monitoring compliance with this Agreement, including experience relevant to monitoring the obligations of this Agreement such as experience with: IT systems, cybersecurity, data privacy, social media platforms, content moderation, designing compliance programs, drafting policies and procedures for large companies, and related national security issues. For each Third-Party Monitor nominee, the Transaction Parties shall submit to the CMAs a detailed professional synopsis of the nominated Third-Party Monitor's experience, as well as any additional information requested by the CMAs. At the time of the nomination and for the duration of a Third-Party Monitor's engagement in connection with this Agreement, the Transaction Parties shall ensure that the nominated Third-Party Monitor has

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

no current or prior contractual, financial, or fiduciary relationship with any of the Transaction Parties or their Affiliates. TTUSDS shall ensure that the Third-Party Monitor, for the duration of its engagement in connection with this Agreement, does not owe any obligation to any of the Transaction Parties or their Affiliates that would limit the independence of the Third-Party Monitor or inhibit the Third-Party Monitor from sharing any information with the CMAs that the Third-Party Monitor or the CMAs deem relevant to ensuring the Transaction Parties' compliance with this Agreement.

16.3 Monitoring Agreement. TTUSDS shall negotiate a monitoring agreement (the "**Monitoring Agreement**") with each Third-Party Monitor. The execution of the Monitoring Agreement shall be subject to the prior non-objection of the CMAs. TTUSDS shall submit a draft of the Monitoring Agreement to the CMAs within ten (10) days following the non-objection of the CMAs to the Third-Party Monitor. If the CMAs do not object in writing to the draft Monitoring Agreement within thirty (30) days following receipt, the lack of action shall constitute a non-objection. If the CMAs object to the draft Monitoring Agreement, TTUSDS shall resolve the concerns to the satisfaction of the CMAs in the CMAs' sole discretion and submit a revised Monitoring Agreement to the CMAs within fourteen (14) days following receipt of the CMAs' comments, subject to the same procedures as the initial draft.

16.4 Within three (3) days following the non-objection of the CMAs to the Monitoring Agreement, TTUSDS shall enter into the Monitoring Agreement with the Third-Party Monitor. TTUSDS shall not amend or terminate the Monitoring Agreement without the prior written consent of the CMAs. TTUSDS shall ensure that the Monitoring Agreement includes at least the following terms:

- (1) the CMAs shall be third-party beneficiaries of the Monitoring Agreement;
- (2) the Third-Party Monitor shall report directly to the CMAs and shall owe a fiduciary duty to the CMAs;
- (3) the Third-Party Monitor shall owe no obligation to any of the Transaction Parties or any other Person that would limit the sharing of information with the CMAs that the Third-Party Monitor or the CMAs deem relevant, in the CMAs' sole discretion, to the Transaction Parties' compliance with this Agreement;
- (4) the Third-Party Monitor shall attend all meetings of the TTUSDS Board and the Security Committee, and otherwise review and observe TTUSDS's and the Security Committee's activities to ensure the security of Protected Data and that TTUSDS and the TTP do not engage in activities that undermine or are inconsistent with this Agreement;
- (5) the Third-Party Monitor shall monitor the relationships, communications, and interactions between ByteDance and its Affiliates, on the one hand, and TTUSDS, on the other hand, to ensure that any such relationships, communications, or interactions do not interfere with TTUSDS's independence and are consistent with this Agreement;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(6) the Third-Party Monitor may, in its sole discretion or at the direction of the CMAs, have the authority to conduct or trigger red or blue-team testing or exercises, the cost of which shall be borne by TTUSDS;

(7) the Third-Party Monitor shall inform the CMAs of any actual or potential violation of this Agreement within one (1) day of becoming aware of the actual or potential violation and shall provide, upon request, any information to the CMAs pertaining to the Transaction Parties' compliance with this Agreement;

(8) the Third-Party Monitor shall provide the CMAs with periodic reports as requested by the CMAs detailing the Transaction Parties' status implementing and complying with this Agreement, including any actual or potential violations of this Agreement;

(9) the Third-Party Monitor shall abide by the CMAs' guidance and protocols in performing its functions under this Agreement;

(10) the Third-Party Monitor shall have, and TTUSDS shall provide the Third-Party Monitor with, the complete ability to operate and have Access within TTUSDS in order to carry out its responsibilities under the Monitoring Agreement;

(11) the Third-Party Monitor shall not disclose any information it obtains in connection with the Monitoring Agreement or its services thereunder to any third party, except for the TTP, Source Code Inspector, Cybersecurity Auditor, or Third-Party Auditor as permitted under this Agreement, without the prior written consent of the CMAs;

(12) TTUSDS shall be responsible for all expenses and fees in connection with the Third-Party Monitor and the Monitoring Agreement;

(13) the Transaction Parties shall provide the Third-Party Monitor with any information that the Third-Party Monitor, in its sole discretion, deems necessary to verify compliance with this Agreement;

(14) upon the request of the CMAs, the Third-Party Monitor shall share with the CMAs any information provided to it from the Transaction Parties; and

(15) the CMAs, in their sole discretion, may direct TTUSDS to terminate the Third-Party Monitor at any time for any reason without approval from the Transaction Parties, and TTUSDS shall promptly, and in any event within three (3) days of such direction, terminate the Third-Party Monitor.

16.5 Non-Retaliation. None of the Transaction Parties shall take any retaliatory actions, including withholding payment, for actions taken by the Third-Party Monitor in order to evaluate and report on compliance with this Agreement.

16.6 Responsibilities. In addition to the responsibilities of the Third-Party Monitor set forth in this Agreement, TTUSDS shall ensure that the Third-Party Monitor takes all steps necessary to continuously monitor the Transaction Parties' compliance with this Agreement,



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

including through: regular interaction with the Transaction Parties' Personnel, including their management and directors, and the Security Officer, Compliance Officer, ByteDance POC, and Technology Officer; inspection of the Transaction Parties' documents, records, policies, and access logs; oversight of TTUSDS's operations involving IT systems, Protected Data, Source Code and Related Files, Content Moderation Processes, and vendors; and any other activities deemed necessary by the Third-Party Monitor to ensure the Transaction Parties' compliance with this Agreement.

16.7 Annual Performance Summary. TTUSDS shall ensure that the Third-Party Monitor submits to the CMAs, within seven (7) days following each anniversary of the Effective Date, a confidential annual performance summary (each, an "**Annual Performance Summary**"). None of the Transaction Parties shall, and the Transaction Parties shall ensure the TTP shall not, request or receive a copy of any Annual Performance Summary. Each Annual Performance Summary shall generally summarize the Third-Party Monitor's actions, decisions, and work performance, as well as the resources devoted to such efforts, from the prior year to carry out its obligations under the Monitoring Agreement, and also shall detail any restrictions experienced in carrying out its obligations. TTUSDS shall ensure that the Third-Party Monitor promptly addresses any questions from the CMAs regarding the Annual Performance Summary.

16.8 TikTok Inc. TikTok Inc. shall share documentation with the Third-Party Monitor, and grant the Third-Party Monitor Physical Access, which may be escorted, as requested by the Third-Party Monitor, in its sole discretion, to facilitate the Third-Party Monitor's assessment of the Transaction Parties' compliance with this Agreement.

## ARTICLE XVII

### CFIUS MONITORING AGENCY REVIEW AND INSPECTION RIGHTS

17.1 Access and Inspection. Upon one (1) day's notice, each of the Transaction Parties shall allow and afford the CMAs access to meet with its Personnel or the Personnel of its Affiliates, and to inspect the books and records, equipment, servers, and facilities, and premises owned, leased, managed, or operated in the United States by such Transaction Party or its Affiliates for the purposes of monitoring compliance with or enforcing this Agreement; *provided* that in exigent circumstances, no advance notice is required. This right to access and inspect extends to the Personnel, books and records, equipment, servers, facilities, and premises of any third-party contractor or agent working on behalf of any Transaction Party or its Affiliates. If any Transaction Party does not possess the authority or capability to afford such access, such Transaction Party shall use best efforts to obtain whatever is required from the third-party contractor or agent for such access to be afforded. Each of the Transaction Parties shall cooperate with the CMAs and promptly provide the CMAs with information as may be requested by the CMAs in their sole discretion to enforce and monitor compliance with this Agreement.

17.2 Access to the TTP. TTUSDS shall ensure, through the MSA, that the TTP provides Physical Access to and tours of its facilities to the CMAs, and facilitates meetings with its Personnel with the CMAs, for on-site reviews or audits during normal business hours to assess the implementation of this Agreement, and allows the CMAs to inspect company records

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

to verify compliance with this Agreement, in each case with no greater than one (1) day's prior notice. TTUSDS shall ensure, through the MSA, that the TTP cooperates with the CMAs and provides the CMAs with all information as may be requested by the CMAs, in their sole discretion, to enforce and monitor compliance with this Agreement.

**ARTICLE XVIII**

**COMPLIANCE**

18.1 Approvals and Authorizations. The Transaction Parties shall obtain and maintain, and shall ensure that their Affiliates obtain and maintain, all legal, statutory, regulatory, or other required authorizations and approvals, including those required by the government of the People's Republic of China, that are necessary to fully satisfy their obligations under this Agreement. Each of the Transaction Parties intends to be bound by all of the obligations under this Agreement regardless of impossibility or foreign compulsion and waives any and all defenses arising out of an inability to obtain any legal, statutory, regulatory, or other required authorization or approval necessary. The Transaction Parties shall promptly report to the Third-Party Monitor and CMAs any non-compliance with this Section 18.1.

18.2 Compliance Policies. Each of the Transaction Parties, in coordination with the Security Committee, the Security Officer, Compliance Officer, or ByteDance POC (as applicable to such Transaction Party), and the Third-Party Monitor, shall adopt and implement, and shall ensure that its respective Personnel follow, a separate compliance policy (each a "**Compliance Policy**") to govern its respective implementation of and compliance with this Agreement. Each Compliance Policy shall be subject to the prior non-objection of the CMAs. Each of the Transaction Parties shall submit a draft of its Compliance Policy to the CMAs within sixty (60) days following the Operational Date, resolve any concerns raised by the CMAs with respect to its Compliance Policy, and submit a revised draft to the CMAs within twenty-one (21) days following receipt of any comments from the CMAs. If the CMAs do not object within thirty (30) days following receipt of any draft of a Compliance Policy, the lack of action shall constitute a non-objection with respect to that Compliance Policy and the relevant Transaction Party shall formally adopt the Compliance Policy within three (3) days following the non-objection of the CMAs. TTUSDS shall ensure that the Security Officer and Security Committee are responsible for the oversight, implementation, and maintenance of the Compliance Policy for TTUSDS.

(1) Each Transaction Party shall ensure that its respective Compliance Policy provides, at a minimum:

(i) procedures for providing, receiving, and responding to information, reports, and requests from the TTP, Third-Party Monitor, and CMAs as required under this Agreement within the specified timelines;

(ii) procedures for coordination between the relevant Transaction Party, its respective Affiliates, the TTP, the Security Committee, the Security Officer, the Content Advisory Council, the Technology Officer, the Source Code Inspector, the

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Third-Party Monitor, the Cybersecurity Auditor, the Third-Party Auditor, and other designees and third parties as applicable and as required under this Agreement;

(iii) procedures and requirements for facilitating all necessary Access by the TTP, Source Code Inspector, Third-Party Monitor, Cybersecurity Auditor, Third-Party Auditor, CMAs, and other third parties as applicable and as required under this Agreement;

(iv) processes for informing and training its Personnel regarding this Agreement;

(v) a notification and reporting policy to govern the prompt reporting of any actual or potential violation of this Agreement to the CMAs;

(vi) guidance on the roles and responsibilities of relevant Personnel to ensure its compliance with this Agreement;

(vii) a policy of non-retaliation for Personnel who report actual or potential violations of this Agreement;

(viii) procedures for periodically reviewing and updating the Compliance Policy as needed to ensure compliance with this Agreement; and

(ix) any other matters identified by the CMAs as necessary to ensure the Transaction Party's compliance with this Agreement.

(2) TTUSDS shall ensure that its Compliance Policy includes procedures for the Security Officer to delegate his or her obligations under this Agreement in circumstances where the Security Officer is unavailable or requires assistance.

18.3 CMA Approvals Required. All protocols and policies required under this Agreement shall be subject to the prior non-objection of the CMAs, unless this Agreement expressly provides otherwise. The Transaction Parties shall not implement protocols and policies, or amend or modify such protocols and policies, without the prior non-objection of the CMAs. The Transaction Parties shall comply with the provisions of all protocols and policies that received the consent, non-objection, or approval of the CMAs under this Agreement. Any violation of the protocols and policies implemented pursuant to this Agreement shall be deemed to constitute a violation of this Agreement, and the failure by the Transaction Parties to obtain authorizations and approvals that are necessary to comply with such protocols and policies shall not excuse a violation thereof.

18.4 Board Resolutions. Each of the Transaction Parties shall ensure that its respective board of directors implements and maintains board resolutions as applicable and as necessary to enable and ensure compliance with this Agreement, and shall submit copies of such board resolutions to the Third-Party Monitor and CMAs within three (3) days following their adoption.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

18.5 Quarterly Meetings. At the request of the CMAs, but not less than once every ninety (90) days unless waived in writing by the CMAs, the Transaction Parties shall meet, and shall ensure through the MSA that the TTP meets, with the Third-Party Monitor and CMAs at a mutually agreed upon time and location or by telephone (each such meeting, a “**Quarterly Meeting**”). At each Quarterly Meeting, the Transaction Parties shall provide, and shall ensure the TTP provides, all information requested, and answer all questions posed, by the Third-Party Monitor and CMAs. The CMAs may, in their sole discretion, exclude one or more of the Transaction Parties from all or part of a Quarterly Meeting. If the CMAs pose written questions to any Transaction Party or the TTP in advance of or following a Quarterly Meeting, such Transaction Party shall submit, and the Transaction Parties shall ensure the TTP submits, written responses to the CMAs within seven (7) days following receipt of the questions, unless otherwise extended by the CMAs.

18.6 Recordkeeping. The Transaction Parties shall ensure that the ByteDance POC, Compliance Officer, Security Officer, and Technology Officer create and maintain adequate records to monitor each of the Transaction Parties' and the TTP's respective compliance with this Agreement. If the TTP is replaced, the Transaction Parties shall ensure that the previous TTP retains copies of any records related to the performance of its obligations in connection with this Agreement and the MSA until advised otherwise by the CMAs.

18.7 Obligation to Report. The Transaction Parties shall: (1) require the ByteDance POC, Compliance Officer, Security Officer, and Technology Officer promptly, and in any event within one (1) day of discovery, to report any actual or potential violation of this Agreement to the Third-Party Monitor and CMAs; and (2) each maintain procedures that require Personnel to promptly inform the ByteDance POC, Compliance Officer, Security Officer, or Technology Officer, as applicable, of any actual or potential violation of this Agreement.

18.8 Defining a Violation. The CMAs may, in their sole discretion, provide interpretive guidance to the Transaction Parties and TTP as to what constitutes an actual or potential violation of this Agreement.

## ARTICLE XIX

### ANNUAL REPORTS

19.1 Annual Reports. Each of the Transaction Parties shall submit, within seven (7) days following each anniversary of the Effective Date, an annual report (each, an “**Annual Report**”) to the Third-Party Monitor and CMAs that summarizes its compliance with this Agreement from the prior year, and includes, with respect to the preceding year:

(1) organizational charts showing the equity and voting interests held in the entity, the dates of any transactions resulting in changes to such equity and voting interests, and with respect to ByteDance, a summary capitalization table identifying all shareholders holding more than one percent (1%) equity interest or voting interest in ByteDance as of the end of each quarter;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

- (2) the address of the headquarters office location of the entity;
- (3) the full name (last, first, middle name) and telephone and email contact information for the ByteDance POC, the Compliance Officer, and the Security Officer, as applicable;
- (4) with respect to ByteDance, an organizational chart demonstrating and explaining which ByteDance Affiliates (including their location) perform work, services, operations, or support in relation to the TikTok U.S. App or TikTok U.S. Platform;
- (5) with respect to TTUSDS: (i) a summary of the funding provided by ByteDance; and (ii) a statement by TTUSDS regarding the sufficiency of such funds to perform its functions under this Agreement;
- (6) a certification of compliance with the hiring protocols required by Section 5.4;
- (7) a headcount of Personnel, and with respect to TTUSDS, a list of the names and titles of Key Management;
- (8) with respect to TTUSDS, the number of Personnel with a prior relationship with ByteDance or its Affiliates, and the percentage of such workforce within TTUSDS;
- (9) with respect to TTUSDS, a summary from the Security Committee of its activities from the prior year pursuant to this Agreement;
- (10) with respect to TTUSDS, a summary from the Content Advisory Council of its activities from the prior year pursuant to this Agreement;
- (11) current Architecture Diagrams, Data Flow Diagrams, and Source Code Review Diagrams;
- (12) a summary of any findings and reports of vulnerabilities designated as high severity or equivalent, including any instance of Malicious Code in the Source Code and Related Files, pursuant to Section 9.6;
- (13) a certification that all changes, updates, alterations, and improvements to the Source Code and Related Files were deployed to the TikTok U.S. App or TikTok U.S. Platform in accordance with the TTP's review and inspection processes pursuant to Section 9.10;
- (14) an update regarding any remediations or alterations to Source Code and Related Files made at the request of the TTP pursuant to Sections 9.10 or 9.15;
- (15) with respect to ByteDance, a certification that all individuals subject to classification as TikTok U.S. Users pursuant to Sections 1.35 and 11.3 are so classified as of the date of the Annual Report;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(16) with respect to TTUSDS, a monthly breakdown of: (i) the total number of registered TikTok U.S. User accounts, and (ii) the number of TikTok U.S. Users who were monthly active users of the TikTok U.S. App;

(17) a summary of any unexpected or unauthorized interactions pursuant to Section 9.17 and whether the circumstances permitting such interactions persist or have been resolved;

(18) a summary of any changes or remediations made to the Recommendation Engine or Content Moderation Processes in response to issues identified by the TTP or Third-Party Monitor pursuant to Section 9.13;

(19) a summary of all changes to Excepted Data and Public Data;

(20) a certification that all Protected Data in the possession of the Transaction Parties is stored and subject to Access controls consistent with the requirements of this Article XI;

(21) with respect to ByteDance, a certification, signed by a duly authorized representative, that none of ByteDance or its Affiliates holds, possesses, or has any Access to Protected Data in violation of this Agreement, or a summary of any findings of and remediations in relation to ByteDance or its Affiliates holding, possessing, or having any Access to Protected Data after the Deletion Date;

(22) a summary of Access instances and compliance efforts in relation to the Limited Access Protocol, including the number of Personnel who used the Limited Access Protocol, their location, the reason for their Access, and the Protected Data Accessed;

(23) with respect to TTUSDS, a summary of compliance efforts in relation to the DPCP, including Training;

(24) with respect to TTUSDS, a summary of any actual or potential violations of the DPCP;

(25) with respect to TTUSDS, updates regarding any remediation efforts in relation to findings from the Cybersecurity Audits conducted pursuant to Article XIV;

(26) updates regarding any remediation efforts in relation to the Audits conducted pursuant to Article XV;

(27) a summary of any challenges experienced in obtaining and maintaining the authorizations and approvals under Section 18.1, including any legal or regulatory changes affecting compliance with this Agreement;

(28) a summary of any actual or potential violations of this Agreement and the remediation efforts in relation thereto;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(29) as applicable, copies of the most recent versions of the DTC Operating Protocols, the Limited Access Protocol, the DPCP, Excepted Data, Public Data, and the Compliance Policies; and

(30) any other subjects identified by the CMAs, in their sole discretion, as relevant to compliance with the Agreement.

19.2 TTUSDS shall ensure, through the MSA, that the TTP submits to the Third-Party Monitor and CMAs, within seven (7) days following each anniversary of the Effective Date, a confidential annual account (each, an “**Annual Account**”) that summarizes the TTP’s compliance with the requirements of this Agreement from the prior year, and includes, with respect to the preceding year:

(1) current Architecture Diagrams, Data Flow Diagrams, and Source Code Review Diagrams;

(2) a description of whether the TTP is sufficiently funded by the Transaction Parties;

(3) a headcount of Personnel of the TTP whose job responsibilities are covered by the MSA and this Agreement;

(4) a certification of compliance with the hiring protocols required by Section 5.4;

(5) the number of Personnel with a prior relationship with ByteDance or its Affiliates, and the percentage of such workforce within the TTP;

(6) a summary of any Physical Access to the DTC withheld by ByteDance or any of its Affiliates and the resolution of the same;

(7) a statement as to the sufficiency of the DTC Operating Protocols in enabling the TTP to fully perform its obligations under the MSA and in connection with this Agreement;

(8) a summary of any interference by ByteDance or any of its Affiliates with the TTP’s Access to the DTC or Source Code and Related Files, or its inspection efforts in the DTC, and the resolution of the same;

(9) a summary of any findings of vulnerabilities designated as high severity or equivalent, including any instance of Malicious Code in the Source Code and Related Files, pursuant to Section 9.6;

(10) any changes to the TTP’s processes, tools, and techniques used for reviewing and inspecting Source Code and Related Files and monitoring and blocking unexpected or unauthorized interactions pursuant to Article IX;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

- (11) any deployment of Source Code and Related Files inconsistent with Section 10;
- (12) a summary of any findings that the Recommendation Engine operated inconsistently with the requirements under Section 9.13;
- (13) an update regarding any remediations or alterations to Source Code and Related Files made at the request of the TTP pursuant to Sections 9.10 or 9.15, and any issues with the Transaction Parties' obligation to address such requested remediations or alterations;
- (14) a summary of any unexpected or unauthorized interactions pursuant to Section 9.17 and whether the circumstances permitting such interactions persist or have been resolved;
- (15) the full name (last, first, middle name) and telephone and email contact information for the Technology Officer;
- (16) any indications that ByteDance or any of its Affiliates possessed or had Access to any Protected Data after the Deletion Date;
- (17) any issues with the restrictions on storage of and Access to Protected Data required under Article XI;
- (18) a summary of Training efforts pursuant to Sections 11.13 and 12.4;
- (19) a summary of any actual or potential violations of this Agreement and the remediation efforts in relation thereto; and
- (20) any other subjects identified by the CMAs, in their sole discretion, as relevant to compliance with the Agreement.

19.3 TTUSDS shall ensure the TTP does not provide any Annual Account to any of the Transaction Parties or their respective Affiliates.

19.4 Each of the Transaction Parties shall promptly submit, and shall ensure the TTP promptly submits, responses and relevant documentation to any requests by the CMAs for further or clarifying information regarding the content of any Annual Report or Annual Account.

**ARTICLE XX**

**CONFIDENTIALITY**

20.1 **Confidentiality.** This Agreement and all information provided by the Parties pursuant to this Agreement and the preceding term sheets will be accorded the confidential treatment required by Section 721(c) and 31 C.F.R. § 800.802 (2020).



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

20.2 Public Summary. Within seven (7) days following the Effective Date, ByteDance and its relevant Affiliates, including TikTok Inc., shall publish a press release and post on the Newsroom of their respective websites and their social media accounts a statement containing the summary of this Agreement at Annex G (the “**Public Summary**”). ByteDance hereby consents that the USG may also publicly disclose the Public Summary. The Transaction Parties shall consult in good faith on any amendments the CMAs may propose to the Public Summary, and the CMAs will consider in good faith any amendments the Transaction Parties may propose to the Public Summary.

20.3 Accuracy Certification. On the Effective Date, each of the Transaction Parties shall submit to the CMAs a certification that satisfies the requirements in Section 721(n) with respect to all information provided to CFIUS from May 27, 2020, through the Effective Date, including in connection with CFIUS Case 20-100 and this Agreement.

## **ARTICLE XXI**

### **REMEDIES**

21.1 Penalties for Violations of the Agreement. Each of the Transaction Parties acknowledges and agrees that if it violates any of the provisions of this Agreement, the Transaction Party may be liable to the United States for a civil penalty (“**Penalty**”), or subject to further action by the United States, consistent with 50 U.S.C. § 4565 and 31 C.F.R. §§ 800.901 and 800.902 (2020) for violations of mitigation agreements and conditions entered into or imposed under Section 721(l). The CMAs, in their sole discretion, may determine whether a violation has occurred, if such violation warrants the imposition of a Penalty or further action, and the appropriate Penalty amount or action, if any. The CMAs may consider a number of factors in determining the amount of a Penalty due for a violation of this Agreement, including the nature of the violation, the materiality of the violation, whether the conduct was willful or reckless, and the damage to the national security resulting from the violation.

21.2 United States Government Remedies. Each of the Transaction Parties acknowledges that if it fails to comply with any of the terms of this Agreement, the CMAs or any other appropriate USG authority may seek any and all remedies available under applicable law, including injunctive or other judicial relief, in addition to the remedies described in Section 21.1 of this Agreement. The taking of any action by the CMAs or other appropriate USG authority in the exercise of any remedy shall not be considered as a waiver by the CMAs or such other USG authority of any other rights or remedies. Nothing in this Agreement is intended to create rights to damages enforceable at law by the Transaction Parties against the USG, or to limit any rights the USG may have under law or regulation or this Agreement.

21.3 Temporary Stop. The Transaction Parties shall prevent, and shall ensure that their respective Affiliates and the TTP prevent, users from accessing the TikTok U.S. Platform (in each case, a “**Temporary Stop**”) within three (3) days following the occurrence of any of the following:

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(1) the failure by the Transaction Parties to establish TTUSDS and ensure that TTUSDS owns or has a license to, and manages, all of the assets and employs all of the Personnel related to the CFIUS Functions by the Operational Date in accordance with Article II;

(2) the failure by the Transaction Parties to ensure that TTUSDS becomes a Transaction Party to this Agreement by the Operational Date as required under Section 2.3;

(3) the failure by the Transaction Parties to execute a final MSA to which the CMAs have non-objectioned in accordance with the timelines under Section 8.2(1); *provided, however*, that a Temporary Stop shall not be required if: (i) the CMAs do not timely respond to an MSA submitted by the Transaction Parties due to a government shutdown; or (ii) the failure to execute the MSA is solely due to the TTP either having (a) failed to execute the MSA in a timely fashion, or (b) unreasonably withheld its consent;

(4) the failure by the Transaction Parties to execute a final MSA to which the CMAs have non-objectioned with a replacement TTP (i.e., not Oracle) in accordance with the timelines under Sections 8.2; *provided, however*, that a Temporary Stop shall not be required if: (i) the CMAs do not timely respond to an MSA submitted by the Transaction Parties due to a government shutdown; or (ii) the failure to execute the MSA is solely due to the replacement TTP either having (a) failed to execute or respond to the MSA draft in a timely fashion, or (b) unreasonably withheld its consent;

(5) notification to the CMAs by TTUSDS or the TTP that ByteDance and its Affiliates have not provided sufficient funds for TTUSDS or the TTP to perform their respective obligations in connection with this Agreement in accordance with Section 2.8 (with respect to TTUSDS) and Section 9.10(3) (with respect to the TTP); *provided that*: (i) TTUSDS or the TTP has first notified ByteDance of the insufficiency and ByteDance has not resolved such insufficiency to the satisfaction of TTUSDS or the TTP, as applicable, within a timely manner; and (ii) after the CMAs have consulted with ByteDance regarding such notification of insufficiency, the CMAs do not provide their written determination that such circumstances do not warrant a Temporary Stop;

(6) notification to the CMAs by the TTP that it has been denied Physical Access to the DTC or Logical Access to review or inspect Source Code and Related Files, or that ByteDance has interfered with the TTP's inspection activities, in violation of the DTC Operating Protocols or Section 9.3, unless the CMAs provide their written determination that such circumstances do not warrant a Temporary Stop;

(7) notification to the CMAs by the TTP of the deployment to the TikTok U.S. App or TikTok U.S. Platform of any changes, updates, alterations, or improvements to the Source Code and Related Files that were not reviewed and inspected by the TTP in accordance with Section 9.10, including the requirement that only Source Code and Related Files for which the SBOM or its equivalent has been digitally signed by the TTP is deployed to the TikTok U.S. App or TikTok U.S. Platform;

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(8) notification to the CMAs by the TTP of the failure to, within 120 days of the Operational Date, incorporate into the Source Code and Related Files for the TikTok U.S. App a protective solution in accordance with Section 9.8;

(9) notification to the CMAs by the TTP, or any results of the U.S. Deletion Audits, Global Deletion Verification, Cybersecurity Audits, Third-Party Audits, or any other audits or monitoring activities performed pursuant to this Agreement, that indicate that ByteDance or any of its Affiliates, intentionally or through gross negligence, did not irretrievably destroy Protected Data as of the Deletion Date or that ByteDance or any of its Affiliates, intentionally or through gross negligence, maintained or maintains Access to Protected Data after the Deletion Date;

(10) notification to the CMAs by the TTP that Protected Data is not stored or subject to Access controls in accordance with Article XI, unless the CMAs provide their written determination that such circumstances do not warrant a Temporary Stop;

(11) the failure by any of the Transaction Parties to remove any individual or entity appointed to any role under this Agreement at the written direction of the CMAs in accordance with the processes for such removals under this Agreement; or

(12) the failure by the Transaction Parties or any of their Affiliates to obtain and maintain all legal, statutory, regulatory, or other required authorizations and approvals, including those required by the government of the People's Republic of China, in a manner that prevents the Transaction Parties or any of their Affiliates from fulfilling their obligations under this Agreement in violation of Section 18.1.

For the avoidance of doubt, as part of a Temporary Stop the Transaction Parties, their Affiliates, and the TTP may allow TikTok users who are not TikTok U.S. Users to access a TikTok platform other than the TikTok U.S. platform.

21.4 Lifting a Temporary Stop. Upon the occurrence of a Temporary Stop, the Transaction Parties shall not resume, and shall ensure the TTP does not resume, allowing users to access the TikTok U.S. Platform until the Transaction Parties have received the written consent of the CMAs to resume such access, upon the CMAs' finding, in their sole discretion, that the event triggering the Temporary Stop has been remedied or otherwise addressed to the satisfaction of the CMAs.

21.5 Suspension of Service. If the Transaction Parties or their Affiliates do not fully implement a Temporary Stop as required under Section 21.44, the CMAs may direct the TTP to suspend, and the Transaction Parties shall ensure through the MSA that the TTP suspends, user access to the TikTok U.S. Platform until the TTP has received the written consent of the CMAs to lift such suspension.

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

**ARTICLE XXII**

**GENERAL PROVISIONS**

22.1 Effectiveness. Except as otherwise specifically provided in this Agreement, the obligations imposed by this Agreement shall take effect immediately upon the Effective Date and shall remain in effect until this Agreement is terminated in accordance with the terms hereof.

22.2 Valid and Binding Obligation. Each Transaction Party agrees that this Agreement constitutes a legal, valid, and binding obligation of such Transaction Party, enforceable against such Transaction Party in accordance with its terms. Each Transaction Party hereby irrevocably and unconditionally waives, to the fullest extent permitted by applicable law, any and all legal, equitable and other defenses to the enforcement of this Agreement or any obligation hereunder it may have (now or in the future) by reason of any illegality or lack of validity or enforceability of this Agreement or any obligation hereunder.

22.3 Release. Upon the execution this Agreement, each of the Transaction Parties, for itself, its administrators, heirs, representatives, successors, or assigns, hereby waives, releases, abandons, and forever discharges CFIUS and its successors, the United States, and any department, agency, or establishment of the United States, and any officers, employees, agents, successors, or assigns of such department, agency, or establishment, from any and all claims, demands and causes of action of every kind, nature, or description, whether known or unknown, which have been, could have been, or could be asserted in connection with CFIUS Case 20-100 or any related orders (including the August 14 Order), regardless of whether they were named in any complaints filed by the Transaction Parties and regardless of whether they were included in the complaint, including any claims for costs, expenses, attorney fees, and damages of any sort.

In connection with such waiver and relinquishment, each of the Transaction Parties acknowledges that it is aware that it may hereafter discover claims presently unknown or unsuspected, or facts in addition to or different from those which it now knows, with respect to the matters released herein. Nevertheless, it is the intention of each of the Transaction Parties, through such release, and with the advice of counsel, to settle and release all such matters, and all claims as described above relative thereto, which heretofore have existed, now exist, or hereafter may exist between the Transaction Parties and CFIUS, the United States, and any department, agency, or establishment of the United States, and officers, agents, employees and former employees, individually or in their official capacities, arising out of or related to any or all of this Agreement, CFIUS Case 20-100, or any related orders (including the August 14 Order); *provided, however*, that nothing herein shall operate to release or discharge any claim for breach of this Agreement.

22.4 Interpretation. The section headings and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of the terms of this Agreement. All references herein to Articles, Sections, and Annexes shall be deemed references to Articles, Sections, and Annexes of this Agreement unless the context shall otherwise require. The words "hereof," "herein," and "hereunder" and words of like import used in this Agreement refer to this Agreement as a whole and not to any particular provision of this

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

Agreement. Whenever the words “include,” “includes,” or “including” are used in this Agreement they shall be deemed to be followed by the words “without limitation.” The word “extent” in the phrase “to the extent” means the degree to which a subject or other thing extends and such phrase shall not mean simply “if.” Whenever any provision in this Agreement refers to action to be taken by any Person, or which any Person is prohibited from taking, such provision shall be applicable whether such action is taken directly or indirectly by such Person. The definitions given for terms in this Agreement shall apply equally to both the singular and plural forms of the terms defined.

22.5 Notice Regarding Legal Representation. The Transaction Parties shall provide notice to the CMAs, including contact information, of any legal representation in connection with obligations under this Agreement, whether outside legal counsel or internal general counsel, within five (5) days following the Effective Date and thereafter within five (5) days following any change to such legal representation.

22.6 Choice of Law. This Agreement shall be governed by and interpreted according to the federal laws of the United States.

22.7 Direct Communications. The Transaction Parties acknowledge that the CMAs may communicate directly with the Security Committee, the ByteDance POC, the Compliance Officer, the Security Officer, the Technology Officer and TTP, the Source Code Inspector, the Third-Party Auditor, the Third-Party Monitor, the Cybersecurity Auditor, and any point of contact designated by the Transaction Parties. The Transaction Parties further acknowledge that the CMAs may communicate directly with any Personnel who initiate or are included on communications with the CMAs regarding this Agreement. These acknowledgments shall in no way prohibit or otherwise restrict the Transaction Parties from consulting with, obtaining advice from, or communicating with the CMAs through counsel.

22.8 Forum Selection. A civil action brought by any Party for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in accordance with Section 721(e)(2) to the extent applicable. If Section 721(e)(2) is not applicable, such civil action shall be brought in the U.S. District Court for the District of Columbia.

22.9 Other Laws. Nothing in this Agreement is intended to limit, alter, or constitute a waiver of:

- (1) any obligation imposed on the Transaction Parties by any U.S. federal, State, or local law;
- (2) any enforcement authority available under any U.S. federal, State, or local law;
- (3) the sovereign immunity of the United States; or

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

(4) any authority or jurisdiction the USG may possess over the activities of the Transaction Parties or their agents located within or outside the United States.

22.10 Conflict with Applicable Laws. In the event that any provision of law to which the Transaction Parties are subject is inconsistent with any provision of this Agreement, the Transaction Parties shall immediately notify the CMAs of the discrepancy and resolve the conflict to the satisfaction of the CMAs.

22.11 Change in Circumstances. If, after this Agreement takes effect, the CMAs or the Transaction Parties believe that changed circumstances warrant a modification or termination of this Agreement (including if the CMAs determine that the terms of this Agreement are inadequate or no longer necessary to address national security concerns), then the Transaction Parties shall negotiate in good faith with the CMAs to modify or terminate this Agreement. For the avoidance of doubt, if any of the Transaction Parties completes an initial public offering or if a sale or transfer of any Transaction Party to any Person that is not a foreign person (as defined at 31 C.F.R. § 800.224 (2020)) occurs, the Transaction Parties may petition the CMAs for a modification or termination (in the event of a requested termination, pursuant to Section 22.15) of this Agreement, which modification or termination shall be in the sole discretion of the CMAs. Rejection of a proposed modification alone does not constitute evidence of a failure to negotiate in good faith.

22.12 Severability. The provisions of this Agreement shall be severable, and if any provision hereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect the validity or enforceability of any other provision of this Agreement or the application of any other provision, which shall remain in full force and effect.

22.13 Waivers. The failure of the CMAs to insist on strict performance of any of the provisions of this Agreement, or to exercise any right granted herein, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by the CMAs of any provision of, or right under, this Agreement shall be valid unless it is in writing and expressly provides for the waiver of a specified requirement under a particular provision of this Agreement. The CMAs shall have the authority to grant or revoke any waiver, exception, consent, or approval in their sole discretion. The Transaction Parties understand and acknowledge that the CMAs will consider requests for a waiver or exception to any provision of this Agreement with a presumption of denial.

22.14 Successors and Assigns. This Agreement is binding upon, and inures to the benefit of, the Transaction Parties and their respective successors and assigns. For purposes of this Agreement, successors and assigns under this Section includes any corporate name changes. No Transaction Party may assign any obligation under this Agreement without the prior written consent of the CMAs. The Transaction Parties shall remain liable for all obligations under this Agreement that are assigned to any other Person. In the event that any Transaction Party effects the transfer, separation, or sale of a material portion of its business operations or assets that are subject to requirements under this Agreement, including by way of a sale of assets, spin-off, split-off, reorganization, or similar transaction, such Transaction Party shall immediately notify

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

the CMAs in writing and, after consultation with the CMAs, the transferee, successor, or acquirer, as applicable, may, without any further action required of the Transaction Parties, execute a joinder agreement under which such transferee, successor, or acquirer, as applicable, takes on the relevant obligations under this Agreement and becomes a Party hereto. In the event that any Transaction Party effects the transfer, separation, or sale of a material portion of its business operations or assets that are subject to requirements under this Agreement to an Affiliate, such Transaction Party shall, at the time of such transaction, cause the relevant Affiliate to execute a joinder agreement under which the Affiliate takes on the relevant obligations under this Agreement and becomes a Party hereto.

22.15 Termination of this Agreement. After this Agreement takes effect, it shall terminate only upon written notice by the CMAs to the Transaction Parties. Termination of this Agreement shall not relieve a Transaction Party from liability for any breach or violation of this Agreement occurring while the Agreement was in effect or for fraud. Article I (Definition of Terms) and Article XXII (General Provisions) shall survive a termination of this Agreement.

22.16 Amendment. This Agreement may be amended only by written agreement signed by all of the Parties.

22.17 Tolling of Deadlines. Any non-objection, consent, or approval provision applicable to the CMAs under this Agreement shall be tolled during a shutdown in federal government operations due to a lapse in appropriations.

22.18 Computing Time. All references to “days” in this Agreement mean calendar days unless otherwise expressly provided. In computing any time period pursuant to this Agreement:

- (1) For any period stated in days:
  - (i) the day of the event that triggers the period is excluded; and
  - (ii) the last day of the period is included, but if the last day is a Saturday, Sunday, or federal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or federal holiday.
- (2) For any period stated in “months,” such period means once every thirty (30) days.
- (3) For any period stated in “quarters,” such period means once every ninety (90) days.
- (4) For any period stated in “years,” such period means once every three hundred and sixty-five (365) days.
- (5) For any period stated “semi-annually,” such period means twice per year.

22.19 Notices. All notices and other communications given or made relating to this Agreement shall be in writing, shall be deemed to have been duly given or made as of the date of

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

receipt, and shall be sent by electronic mail addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such other addresses as the applicable Party may designate in accordance with this Section:

If to the CMAs:

[XXX]

If to TTUSDS:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

If to TikTok Inc.:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

If to TikTok Ltd.:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

If to ByteDance:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

22.20 Entire Agreement. This Agreement, together with any Annexes and Exhibits hereto, constitutes the entire understandings of the Parties hereto and supersedes all prior agreements or understandings with respect to the subject matter hereof.

22.21 Counterparts. This Agreement may be executed in one (1) or more counterparts, including portable document format (.pdf) or other electronic counterparts, each of which shall be deemed an original, but all of which together shall be deemed to constitute one and the same agreement.



**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

This Agreement is executed on behalf of the Parties:

ByteDance Ltd.

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name:  
Title:

TikTok Ltd.

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name:  
Title:

TikTok Inc.

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name:  
Title:

TTUSDS

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name:  
Title:

For [•]

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name:  
Title:

**CONFIDENTIAL PURSUANT TO 50 U.S.C. § 4565  
EXEMPT FROM DISCLOSURE UNDER 5 U.S.C. § 552  
Parties' Draft as of 8/23/22**

For [•]

Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name:

Title:

For [•]

Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name:

Title:

**Updated Definition of Terms Used in Annexes A and B**

This table lists and defines various terms used in the descriptions laid out in Annexes A and B to the Term Sheet, related to Engineering and Business Related data and Interoperability data, respectively. Note that consistent with the categories laid out in Annex A, this data will be aggregated and will not contain identifiable information.

<b>Term</b>	<b>Definition</b>
<i>3P data sharing requested</i>	advertising engagement behavior (e.g., views and clicks of an advertisement) that is shared with third-party partners to measure advertising performance
<i>Account property</i>	user account data (e.g., register time, signature, number of videos published, number of followers)
<i>Account status</i>	indicates the status of the user account (e.g., registered, unregistered, banned)
<i>Action placement and history</i>	data on each step of the user engagement funnel (e.g., how many users start recording video, then edit their video, then publish their video); allows measurement of the total click-through rate and loss rate of each step
<i>Action source user attributes</i>	user behavior attributes (e.g., 'live_duration_d30_avg_layer_byda_v1', which is calculated by the host's 30 day average live streaming duration time)
<i>Activity attributes</i>	data related to the attributes of live streaming activity (e.g., activity name, activity time)
<i>Addebug</i>	data from each module in the advertising process that enables advertising optimization
<i>Ads attributes</i>	data related to the attributes of an advertising campaign (e.g., advertising objective, targeting criteria, bidding settings, delivery schedule)
<i>Ad property</i>	data related to the creative aspects of an advertising campaign (e.g., content, graphics, text, comments)
<i>Ads experiment attributes</i>	data related to the attributes of an advertising campaign experiment (e.g., advertising objective, targeting criteria, bidding settings, delivery schedule, experiment details)
<i>Ads review attributes</i>	indicates whether a specific advertisement has passed or failed the advertisement review process and the associated reason (e.g., "rejected because of violence content")
<i>Ads tracking option</i>	indicates an option for sending engagement behavior data between users and advertisements to third-party partners (e.g., domain name)
<i>Adset property</i>	Same as "Ad property"

<i>Agency property</i>	segmented user acquisition metrics (e.g., installs, retention, cost) by advertising agency names
<i>Anchor fans range</i>	a range indicating the number of fans identified in a live-streaming anchor (an anchor is a special link on a video that enables users to enter an application or website if the user is interested in a deeper exploration of related content within a video. It's composed of 3 basic parts: icon, title, landing page)
<i>App attributes</i>	app installation package attributes (e.g., app version, app name)
<i>App page</i>	indicates which of the two potential app homescreens is designated (i.e., the "For You" page or the "Following" page)
<i>App property</i>	basic information of the application (e.g., app id, app version, iOS/Android)
<i>Arbit trigger</i>	indicates whether a push is triggered by Arbit (Arbit is the name of a system that triggers content/video pushes by the push algorithm)
<i>Basic user interaction</i>	commonly used aggregated metrics of user engagement with advertisements (e.g., impression, click, video play)
<i>Bid</i>	offer by an advertiser of a specific price for a unit of result for their advertisement groups (e.g., a system generated id which equates to "paying \$15 for 1K impressions")
<i>Bidding (settings)</i>	settings that allow advertisers to set their bid strategy (for further information on bid strategies, see <a href="https://ads.tiktok.com/help/article?aid=9685">https://ads.tiktok.com/help/article?aid=9685</a> )
<i>Campaign property</i>	segmented paid advertisement metrics by campaign names
<i>Channel</i>	type of subdivision for media source traffic (e.g., Google can be divided into search channel and YouTube channel)
<i>Channel property</i>	same as "Channel"
<i>Client interaction</i>	actions taken by a user through the TikTok app or website (e.g., like, save, favorite, watch video to completion)
<i>Comment push off/on</i>	indicates whether a user has turned on push notification for comments
<i>Content type</i>	type of content (e.g., video, music, user card, comment, live streaming)
<i>Conversion (settings)</i>	settings that allow advertisers to set a conversion goal for their advertisement groups from the conversion types
<i>Conversion type</i>	type of conversion goal advertisers set for their advertisement groups (e.g., app download, installation, activation, registration)
<i>Coarse location</i>	information that describes the location of a device with lower resolution than a latitude and longitude with three or more decimal places

<i>Comment attributes</i>	action types such as comment posts and comment likes; comment characteristics (e.g., whether the comment is spam, whether the comment is posted by friends)
<i>Creative</i>	reference to the specific images or videos that are presented to users, to facilitate evaluation of how users responded to that specific image or video advertisement
<i>Creative property</i>	creative characteristics (e.g., creative media types, including image, video and text)
<i>Creator power of influence</i>	measurement of creator's influence (e.g., how many followers, frequency of engagement)
<i>Customer service attributes</i>	segment users by customer service-related attributes (e.g., feedback types such as bugs, suggestions, and help)
<i>Device attributes</i>	characteristics of the device being used to access the TikTok platform (e.g., make, model, OS type, OS version)
<i>Device health statistics</i>	statistics that can be used to check whether the app resource usage is normal (e.g., CPU utilization, memory usage, battery usage)
<i>Digg push off/on</i>	indicates whether a user has turned on system notifications for likes their content receives
<i>E-commerce product attributes</i>	characteristics of an e-commerce product (e.g., product category, price range)
<i>Engineering Shard Group</i>	identifies from which “shards” given data originated (i.e., for systems too large to host in a single machine, the system is split into different shards, each shard handles different parts of data and each shard consists of several processes). This identifier allows the engineering team to identify if there are certain shards/systems that are not meeting performance expectations.
<i>Evaluation metrics</i>	metrics which can be used to evaluate the performance of AI models or other technical optimizations (e.g., network optimization)
<i>Execution attribute</i>	tag for moderation purposes (e.g., pornography, hate speech, language) to facilitate queueing for review
<i>Experiment group</i>	randomized sampling of users, with no identifying information (will only ever be generated by the TTP, with no ByteDance/TikTok insight into identifiable user data)
<i>Flow control</i>	attributes related to a mechanism for controlling how many and how fast advertisements should be delivered to users; there is a module in the advertisements delivery system to enable the mechanism
<i>Follow new story push off/on</i>	indicates whether a user has turned on push notifications for following of new stories
<i>Follow push off/on</i>	indicates whether a user has turned on push notifications for follows

<i>General statistics</i>	general statistics (e.g., sum, average, standard deviation)
<i>Geo</i>	geographic information (i.e., country, state, county, city, Nielsen designated market area)
<i>Gift attributes</i>	attributes of a live streaming gift, which users in the audience can send to a live streaming host (e.g., gift name, gift price)
<i>Grade level</i>	user's age range
<i>Growth attributes</i>	attributes related to how TikTok has acquired a user (e.g., advertising campaign id, media source, new user status, activation date)
<i>Impression</i>	one measure of users' engagement with the advertisement (e.g., user clicked like, user watch advertisement until completion)
<i>Im push off/on</i>	indicates whether a user has turned on push notifications for instant messages
<i>Inner or out app push</i>	whether a push is an in-app notification or system push notification
<i>IVT</i>	abbreviation for "invalid traffic;" it relates to advertising traffic that has been identified through in-house or third party solutions as highly unlikely to be human-triggered and therefore should not be considered in aggregated reporting for advertisers
<i>Labeling results</i>	video labeling flag by a content moderator (e.g., violation, video not recommended, or pass)
<i>Lift or Lift_study</i>	one measure of the performance of an advertisement (e.g., percentage increase in advertiser conversions attributable to the advertisement)
<i>Live attributes</i>	attributes associated with live streaming activities (e.g., the mode of live streaming: Open Broadcaster Studio (OBS) Studio, live studio)
<i>Live inner push off/on</i>	indicates whether a user has turned on push notifications for live onsite events
<i>Live push off/on</i>	indicates whether a user has turned on push notifications for live offsite events
<i>Media property</i>	advertisement platforms (e.g., Google ads, Facebook ads, Twitter ads)
<i>Mention push off/on</i>	indicates whether a user has turned on push notifications for mentions
<i>Network environment</i>	indicates whether a user is accessing the TikTok platform through a wifi network or a cellular data network; the name and address of the network is not provided
<i>Order attributes</i>	attributes related to a user recharge or refund order for sales via the TikTok platform (e.g., recharge reason, order status)
<i>Order status</i>	indicates whether sales orders via the TikTok platform have been placed, paid, shipped, delivered, returned/refunded, or cancelled
<i>Play event</i>	event of a user playing a video in the application

<i>Pbole</i>	indicates whether user and their device information is stored in pBole; pBole is an internal system that is responsible for push-related activities
<i>Pbole pushable</i>	indicates whether user and device information can be pushed through pBole.
<i>Performance event</i>	designation of an event where a user encounters a problem (e.g., delay, lag, crash (used for improvement/optimization purposes))
<i>Placement (settings)</i>	settings that allow advertisers to determine where their ads will be delivered (e.g., TikTok landing page, interspersed in “For You” feed)
<i>Predicted age group</i>	user’s age group predicated by AI model
<i>Predicted gender</i>	user’s gender predicted by AI model
<i>Prediction model</i>	AI models used to predict what users will like; prediction model performance measurements, commonly referred to as “area under the curve”, represents how successful the AI model is
<i>Pricing (settings)</i>	settings that allow advertisers to determine the goal on which they will be charged; the possible values are: 1: cpm (Cost Per Mille); 2: cpc (Cost Per Click); 3: cpt (Cost Per Time); 4: noc (self-operated non-charging); 5: gd (Guaranteed delivery); 6: ocpc (Optimization Cost Per Click); 7: cpa (Cost Per Action); 8: ocpm (Optimization Cost Per Mille); 9: cpv (Cost Per View)
<i>Promoted ad attributes</i>	attributes of the promoted mobile apps (e.g., app name registered in TikTok ads platform, the event type that takes place in the app)
<i>Promoted product</i>	types of advertising products that TikTok provides (e.g., dynamic product ads, coupon ads)
<i>Psort cover</i>	indicates whether the pSort system has user or device information; pSort is an internal system for algorithm-based push notifications
<i>Psort send</i>	indicates whether the pSort systems sends push notifications to a user
<i>Push attributes</i>	attributes of the push notification (e.g., priority level, timeframe)
<i>Push type</i>	type of push notification
<i>PV</i>	abbreviation for “page views”
<i>Query</i>	designation for any specific user search term; to request aggregated results associated with that term (e.g., how many users have searched for “superbowl2020”, “charlidamelio”, “addisonre”, etc. during a specific period)
<i>Reason</i>	designation indicating reason for failure of a backend request (e.g., backend service is not available; invalid request)
<i>Recommend video push off/on</i>	indicates whether a user has turned on push notification for recommended videos



<i>Referral sources</i>	website or app that led the user to the TikTok platform (e.g., a user searches for a topic using Google and one of the search result is a link to a TikTok video; “Google” would be the referral source)
<i>Referral user attributes</i>	attributes of users who referred other users (e.g., referral action date, activation channel, activation date of referred user, and other common user attributes such as operating system, state, region)
<i>Rule_id</i>	internal unique id of security control rules
<i>Rule hits</i>	number of positive hits of a specific security control rule
<i>Search attributes</i>	characteristics of search behavior within the TikTok app.(e.g., where within the app the search activity is occurring and the document type clocked after a given search)
<i>Search channel attributes</i>	attributes of users acquired through search channel (e.g., search source, search keyword, if search page has result)
<i>Search scenario</i>	source/channel for the initiation of the search within the TikTok app (e.g., tab at the bottom of the app where the searches can be initiated like “Discover” tab, “Video” tab, and “Music” tab)
<i>Search user type</i>	type of users who performed search (e.g., registered user, unregistered user)
<i>Security attributes</i>	Security attributes refer to security control decisions (e.g., pass, observe and block) and security engineering features (e.g., type of event, past security verdict of account, account signup channel)
<i>Shop</i>	seller/shop that is providing the merchandise (e.g., Nike official)
<i>Shopping process flow</i>	designation for the steps in the in-app shopping process (e.g., viewing, added to cart, review cart, checkout)
<i>Stages of delivery system</i>	internal steps in the ads delivery pipeline (e.g., target setting mapping, regional risk-control, ads frequency control, ads-blocking, ecpm ranking)
<i>Status of followship</i>	user tier by number of followers
<i>Story interaction push off/on</i>	indicates whether a user has turned on push notifications for story interactions
<i>Survey attributes</i>	attributes of the user completed survey (e.g., questionnaire ID, questionnaire name, questionnaire type – long text v. multiple choice)
<i>Tag status &amp; availability</i>	tags for the audience targeting implementation; they indicate the status and availability of the tag generating process
<i>Targeting (settings)</i>	settings that allow advertisers to set to whom they want their ad groups delivered; could be a combination of targeting attributes and their values (e.g., “female 18-24 users who are in NYC”)
<i>Targeting attributes</i>	attributes that are associated with a group that the advertiser wants to target (e.g., age range, gender, country and region, device platform)
<i>Tasks</i>	tasks assigned to a content moderator (e.g., labeling a video)

<i>Task attributes</i>	attributes of a live streaming task, which the operator can configure in the operation platform (e.g., task name, task time, task config)
<i>Tbase</i>	indicates whether a user device is in Tbase; Tbase is an internal system that stores user device information for content delivery
<i>Ttpush</i>	indicates whether a user or device is in TTPush; TTPush is an internal system for push notifications
<i>Union attributes</i>	attributes of a live streaming union, which is a business organization managing a list of live streaming hosts (e.g., union name, country of a union)
<i>User active history</i>	user’s historical engagement with the app (e.g., number of days the user is active in the app)
<i>User attributes</i>	segment users by source (e.g., paid ads, referral, organic); location (e.g., regions, countries, states); behaviors (e.g., lifetime, active date)
<i>User properties</i>	same as “User attributes”
<i>User grouping</i>	same as “User attributes”
<i>User Scenario</i>	designation for the relevant page of the TikTok app (e.g., “For You” feed, profile, search)
<i>UV</i>	abbreviation for “unique visitor” or “unique user”; refers to a person who has visited the website at least once and is counted only once in the reporting time period, even if through multiple sessions
<i>UX performance metrics</i>	user experience performance data (e.g., latency, time to load first video, crash metrics)
<i>Video attributes</i>	designation for certain video characteristics (e.g., video effects, filters, hashtags, music)
<i>Video content attribution</i>	technical attributes of the video content (e.g., height, width, resolution, duration, music, album)

ANNEX A – Engineering and Business Related Metrics

# Material Under Seal Deleted

# Material Under Seal Deleted

# Material Under Seal Deleted

# Material Under Seal Deleted

ANNEX B – Interoperability Data



# Material Under Seal Deleted

Annex C – E-Commerce Data

# **Material Under Seal Deleted**

Annex D – Form of Joinder Agreement for TTUSDS

Annex E – Feature Categories as of the Effective Date

ANNEX F – List of ByteDance Competitors

ANNEX G – Public Summary



Prepared by the research staff of the  
U.S.-China Economic and Security Review Commission (USCC.gov)

April 14, 2023

## Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes

Nicholas Kaufman, Policy Analyst, Economics and Trade

This Issue Brief details the challenges posed by Chinese “fast fashion” platforms, including exploitation of trade loopholes; concerns about production processes, sourcing relationships, product safety, and use of forced labor; and violations of intellectual property rights. These platforms primarily rely on U.S. consumers downloading and using Chinese apps to curate and deliver products. The primary focus of this Issue Brief is first mover Shein, about which the most data is available, with additional discussion of Temu, which has rapidly expanded its U.S. market presence in the past year. These firms’ commercial success has encouraged both established Chinese e-commerce platforms and startups to copy its model, posing risks and challenges to U.S. regulations, laws, and principles of market access.

### Key Findings

Founded in 2008, Shein has emerged as a leading player for “fast fashion”<sup>\*</sup> consumers. Shein and similar companies work to market new, fashionable clothes from online and celebrity trends and deliver them quickly to consumers. Amid increased online purchases and fast-shifting trends influenced by social media, fast fashion has grown to a \$106.4 billion industry as of 2022.<sup>† 1</sup> Using data analysis of its users’ search history and a consolidated and high-speed supply chain, Shein has outpaced competitors—including Zara and H&M—to take a dominant position in the U.S. market, a business model that other Chinese firms are seeking to replicate.

Numerous controversial practices have supported Shein and other Chinese e-commerce firms’ rapid growth. Investigations in 2022 alleged that Shein failed to declare that it had sourced cotton from Xinjiang for its products, a violation of the Uyghur Forced Labor Prevention Act. These claims are exacerbated by further reports of illegal labor conditions among the suppliers of Chinese fast fashion firms as well as findings that Shein products pose

<sup>\*</sup> Fast fashion is defined as cheap, trendy clothing that samples ideas from the catwalk or celebrity culture and turns them into garments at high speed to meet emerging consumer demand. Katherine Saxon, “Fast Fashion 2021 Guide – What It Means, Problems, and Examples,” *Fibre2Fashion*, August 2021. <https://www.fibre2fashion.com/industry-article/9163/fast-fashion-2021-guide-what-it-means-problems-and-examples>.

<sup>†</sup> China has accounted as the largest supplier to the U.S. apparel market through 2021; Beth Wright, “ANALYSIS: China Market Share of US Apparel Imports Rises after Four-Year Lull,” *Just Style*, March 4, 2022. <https://www.just-style.com/features/analysis-china-market-share-of-us-apparel-imports-rises-after-four-year-lull/>.

**Disclaimer:** The U.S.-China Economic and Security Review Commission was created by Congress to report on the national security implications of the bilateral trade and economic relationship between the United States and the People’s Republic of China. For more information, visit [www.uscc.gov](http://www.uscc.gov) or follow the Commission on Twitter at @USCC\_GOV.

This report is the product of research performed by professional staff of the U.S.-China Economic and Security Review Commission (USCC) and was prepared to support the ongoing research and deliberations of the Commission. Posting of this report to the Commission’s website is intended to promote greater awareness and understanding of developing issues for congressional staff and the public, in support of the Commission’s efforts to “monitor, investigate, and report” on U.S.-China economic relations and their implications for U.S. national security, as mandated by Public Law 106-398 (as subsequently modified in law, see [uscc.gov/charter](http://uscc.gov/charter)). The public release of this document does not imply an endorsement by the Commission, any individual Commissioner, or the Commission’s other professional staff, of the views or considerations raised in this staff-prepared report.



health hazards and environmental risks. Shein and several other Chinese fast fashion firms have also faced a high volume of copyright infringement accusations and lawsuits for intellectual property (IP) rights violations.

Shein and similar companies present a range of challenges to U.S. interests, including difficulties monitoring supply sources and obstacles in ensuring fair market practices with U.S. competitors. These companies also exploit trade de minimis import exemptions, through which firms make shipments to the United States that are below an \$800 value and are therefore not subject to import duties. Taken together, Shein and similar firms serve as a case study of Chinese e-commerce platforms outmaneuvering regulators to grow a dominant U.S. market presence.

## Shein's Business Model: User Data and Supply Chain Integration

Shein's business model is distinguished by its reliance on tracking and analyzing user data. Founded by Chris Xu, a Chinese national with a background in search engine optimization, Shein draws on customer data and search history with the assistance of artificial intelligence (AI) algorithms to discern emerging fashion preferences and patterns.<sup>2</sup> With these rapid insights, Shein can begin manufacturing and delivering clothes to market ahead of competitors. To aid its data collection, the company's app also requests that users share their data and activity from other apps, including social media, in exchange for discounts and special deals on Shein products.<sup>3</sup>

While Shein has a supplier model built on tech-driven insights, it has struggled to protect user data. New York State fined Shein's owner, Zoetop—a Hong Kong-based LLC that owns Shein and sister company ROMWE—\$1.9 million in 2022 for mishandling credit card and other personal information following an investigation of a 2018 cyberattack that exposed the user data of 39 million accounts, including 800,000 users in New York.<sup>4</sup> The office of the New York attorney general found that Zoetop had misled consumers about the extent of its data breach, had notified “only a fraction” of affected users that data credentials had been compromised, and had not reset the login credentials or otherwise taken steps to protect many of the exposed accounts.<sup>\* 5</sup>

Aside from anticipating trends, Shein's success also hinges on its ability to deliver products to consumers on a compressed timeline and at low cost. The company's integrated supply chain enables it to bring clothes to market in about five to seven days, when its competitors may take three weeks or longer.<sup>6</sup> While Shein initially marketed products it purchased from third parties, it has built a sizeable exclusive supplier base in Guangdong Province, allowing it to improve manufacturing and delivery times.<sup>†</sup> According to a 2021 report by United Kingdom (UK)-based Channel 4, nearly half of the clothing suppliers in Guangzhou are partnered with Shein.<sup>7</sup> This control over its own supply enables Shein to produce small batches of apparel quickly, rather than the typical practice of placing bulk orders, as U.S. firms do. Shein may produce as few as 50 pieces of clothing in its first production batch in order to accelerate delivery to buyers.<sup>8</sup>

Although founded in China, Shein does not sell domestically, instead marketing products exclusively abroad. Its presence has grown considerably in the United States over the last three years. With an aggressive digital and social media advertising campaign complemented by the expansion of online buying during the COVID-19 pandemic, Shein's market share of fast fashion sales in the United States rose from 18 percent in March 2020 to 40 percent in March 2022.<sup>9</sup> By November 2022, Shein accounted for 50 percent of all fast fashion sales in the United States, ahead of brands H&M (16 percent) and Zara (13 percent).<sup>10</sup> After surging past Tiktok, Instagram, and Twitter to briefly become the most downloaded app in the United States in May 2022, Shein maintained its growing popularity,

---

\* Of the leaked New York resident accounts, 375,000 were via Shein accounts, and 255,294 New York residents were not notified about the breach, according to the New York attorney general's office. Zoetop did not detect the intrusion until it was later notified by its payment processor that its systems appeared to have been compromised. In addition, Zoetop's public statements about the breach misrepresented the breach's size and scope. For example, Zoetop falsely stated that only 6.4 million consumers were affected by the breach and that the company was working notifying all of the impacted customers. Zoetop also represented, falsely, that it “ha[d] seen no evidence that [customer] credit card information was taken from [its] systems.” Two years later, Zoetop found customer login credentials for ROMWE accounts available on the dark web. New York State Office of the Attorney General, *Attorney General James Secures \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers' Data*, October 12, 2022. <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop>.

† Shein utilizes a distributed network of suppliers across Guangdong Province and has steadily accumulated more than 200 contracted manufacturers near its major shipping hub in Guangzhou. These contractors are directly fed direction from Shein on production details and batch size in order to produce Shein products on an expedited timeline. Lora Jones, “Shein: The Secretive Chinese Brand Dressing Gen Z,” *BBC*, November 9, 2021. <https://www.bbc.com/news/business-59163278>.

finishing the year as the most downloaded platform for beauty and fashion across the U.S. application marketplace.<sup>11</sup> With 27 million downloads, Shein had more than double second-place Nike's 12.5 million downloads.<sup>12</sup>

The experience of Shein's expanding presence in the United States runs counter to that of U.S. e-commerce platforms in China.\* Major digital and e-commerce firms face staunch regulatory barriers establishing operations, including onerous censorship restrictions and stiff legal regulations regarding cybersecurity.<sup>13</sup> These market and non-market barriers forced Amazon to close down its Chinese marketplace in 2019.<sup>14</sup>

### Chinese e-Commerce on U.S. Social Media

Social media increasingly plays a central role in the marketing of goods to U.S. consumers. In 2022, U.S. firms spent an estimated \$56 billion promoting their products on social networks.<sup>15</sup> Half of Gen Z (18–25) and Millennial (26–41) consumers made purchases directly via social media platforms, according to the 2022 U.S. Digital Trust Survey.<sup>16</sup>

Among Chinese e-commerce firms, Shein and Temu—another China-based fast fashion app—are particularly well positioned to exploit social media platforms as a key conduit to U.S. consumers. Shein has more than 250 million followers across its social media channels.<sup>17</sup> The “#shein” TikTok tag has over 3.3 billion views.<sup>18</sup> Temu has invested heavily in social media marketing, purchasing 8,900 ads across Meta platforms in January 2023 alone.<sup>19</sup>

Both Shein and Temu partner closely with social media influencers. In a standardized application process on its website, Shein seeks influencer partnerships in exchange for shopping perks, bonuses, and exposure to its “community of 1M+ followers.”<sup>20</sup> Temu, which requires applicants to have at least 300 followers, similarly offers shopping perks and rewards.<sup>21</sup> Influencers are encouraged to post “haul” videos of Shein and Temu products on U.S. social media platforms, where they are shown trying on clothes and other accessories and recommending products to followers.

## Controversies in Shein's Business Practices

Several concerning patterns and practices have aided Shein's market approach.

- *Forced labor.* Shein cotton apparel sourcing practices appear to be in direct violation of the Uyghur Forced Labor Prevention Act. A Bloomberg investigation published in November 2022 cross-referenced climate and weather signatures on cotton fabrics used in clothing from Shein to determine that they originated in Xinjiang.<sup>†</sup><sup>22</sup> The Uyghur Forced Labor Prevention Act bans the use of Xinjiang cotton in imported clothing unless the supplier can definitively prove that the cotton was not a product of forced labor, a step that Shein has not taken.<sup>‡</sup><sup>23</sup>
- *Other exploitative labor practices and labor violations.* Outside of concerns about forced labor, a 2022 investigation by Channel 4 found a pattern of labor practice violations at Shein-affiliated factories in Guangzhou.<sup>24</sup> In one factory, workers were paid the equivalent of \$556 a month to make 500 garments a

\* While no U.S. fast-fashion company has attempted market expansion into China comparable to Shein or Temu's inroads in the U.S. market, the experience of U.S. e-commerce companies in China is noteworthy due to the Chinese government's strict regulation of all internet companies and expanded control of the e-commerce market. Bien Perez, “China's E-Commerce Crackdown: Timeline of Beijing's Actions to Bring Tech Giants in Line with National Policy,” *South China Morning Post*, November 22, 2021. <https://www.scmp.com/tech/policy/article/3156719/chinas-e-commerce-crackdown-timeline-beijings-actions-bring-tech-giants>.

† Bloomberg contracted Agroisolab GmbH, a lab in Germany, to test the items using stable isotope analysis. This process measures variations in the isotopes of carbon, oxygen, and hydrogen in the cotton's fibers to determine the climate characteristics and altitude of the region where it was grown. Shein's cotton was compared with two fabric samples from Xinjiang and. The first batch of Shein garments tested, which included pants and a blouse, matched the Xinjiang samples with only slight variations. Sheridan Prasso, “Shein's Cotton Tied to Chinese Region Accused of Forced Labor,” *Bloomberg News*, November 20, 2022. <https://www.bloomberg.com/news/features/2022-11-21/shein-s-cotton-clothes-tied-to-xinjiang-china-region-accused-of-forced-labor?sref=mxblZFb4>.

‡ Xinjiang Province is the source of 87 percent of Chinese cotton as of 2021. U.S. importers bought about \$8.4 million worth of cotton products from China in 2022, despite restrictions; Sheridan Prasso, “Shein's Cotton Tied to Chinese Region Accused of Forced Labor,” *Bloomberg News*, November 20, 2022. <https://www.bloomberg.com/news/features/2022-11-21/shein-s-cotton-clothes-tied-to-xinjiang-china-region-accused-of-forced-labor?sref=mxblZFb4>.

day.<sup>25</sup> Workers had their first month's pay withheld in order to ensure worker retention. In another factory, workers had no base pay and were instead paid 4 cents a garment. These workers were fined heavily for mistakes in stitching or sewing.<sup>26</sup> The report further found workers in Shein factories working 18-hour workdays with one day off a month, clear violations of both Chinese labor laws and Shein's own supplier Code of Conduct.<sup>27</sup> Shein has faced other recent accusations of violating labor laws. Reuters reported in 2021 that Shein made false statements and lacked disclosures regarding its labor conditions, in violation of the UK's Modern Slavery Act.<sup>28</sup> A 2021 report from Public Eye, a Swiss Human Rights watchdog, described six Shein-affiliated factories without suitable fire exits and workers placed on extended working hours of about 75 hours a week with no overtime pay, another violation of Chinese labor law.<sup>29</sup>

- *Health hazards.* The environmental and health impacts of Shein products are also facing scrutiny. A CBC Marketplace investigation found Shein clothing materials containing high levels of potentially hazardous chemicals, including lead, perfluoroalkyl (PFA), and phthalates.\*<sup>30</sup> Health Canada tested a Shein jacket for toddlers and found it to have 20 times the amount of lead considered safe for children, while a purse from Shein contained over five times the accepted level for children.<sup>31</sup> Environmental group Greenpeace also released a study alleging that various chemicals used in Shein products exceeded the level permitted by EU regulations.<sup>32</sup>
- *Climate and environmental impact.* The UN Environmental Program estimates that due to its high-volume output, the fashion industry is responsible for 10 percent of annual global carbon emissions, more than all international flights and maritime shipping combined. At its current rate of growth, the fashion industry's greenhouse gas emissions will surge more than 50 percent by 2030.<sup>33</sup> Shein and other fast fashion platforms are exacerbating this trend by supplying higher volumes of cheaply produced clothing. A Bloomberg report found that Shein products contain 95.2 percent new plastics rather than recycled materials, while the large volume of shipments and low reuse rate among Shein products increases textile waste.<sup>34</sup> Good on You, which ranks the environmental impact of fashion companies, gave Shein its lowest rating.<sup>35</sup>
- *Copyright infringement.* Shein and other Chinese e-commerce platforms and their suppliers have been met with numerous claims that they consistently violate U.S. IP law, with the *Wall Street Journal* reporting in 2022 that Shein in particular had over 50 outstanding federal cases over three years levied against it alleging trademark or copyright infringement.<sup>36</sup> In a June 2021 case, AirWear International, the parent company of shoe seller Dr. Martens, filed a lawsuit against Shein for its alleged "clear intent to sell counterfeits" and for copying the company's designs.<sup>37</sup> Complaints and cases against Shein range from major U.S. designers and retailers like Ralph Lauren to independent artists who claim Shein suppliers have used their designs on Shein clothing without permission. Independent designers who earn more of their income online are particularly vulnerable, as they have fewer resources with which to pursue legal action against Shein and its suppliers.<sup>38</sup>
- *Avoiding tariffs and customs inspections.* Shein clothing and accessories average about \$11 per item.<sup>39</sup> This under-market pricing means Shein is exempt from the standard 16.5 percent import duty and 7.5 percent tariff specific to China.<sup>40</sup> De minimis packages are also exempt from customs inspection, allowing Shein to ship directly to consumers and helping the company avoid scrutiny over its cotton sourcing. Shein also benefits from a tax break in China: in response to the escalating U.S.-China trade dispute, in 2018 China waived export tariffs for direct-to-consumer businesses.<sup>41</sup>

---

\* Research involving humans suggest that exposure to high levels of these PFAs and phthalates may pose risks of liver and kidney damage; Agency for Toxic Substance and Disease Registry, "What are the health effects of PFAS?" *Center for Disease Control*, November 1, 2022. <https://www.atsdr.cdc.gov/pfas/health-effects/index.html>. New Jersey Department of Health, *Hazardous Substance Fact Sheet*, May 2010. <https://nj.gov/health/eoh/rtkweb/documents/fs/1454.pdf>.

### De Minimis Packages from China Evade Tariffs

Chinese e-commerce's growth in the United States has been aided by exploitation of favorable import regulations, especially the high de minimis threshold for U.S. customs inspection and tariffs. A de minimis threshold demarcates the value below which goods are considered too small to be subject to tariffs or most inspections. In the United States, this threshold was raised from \$200 to \$800 in 2016.<sup>42</sup> By contrast, it is roughly \$7 (renminbi [RMB] 50) in China.<sup>43</sup>

A sizeable majority of de minimis packages, which increased from 410.5 million packages in fiscal year (FY) 2018 to 685.1 million packages in FY 2022, came from China.<sup>44</sup> This correlates closely with the rise of e-commerce deliveries from China to the United States.<sup>45</sup> Shipments of de minimis packages from China in 2021 were about seven times the amount of Canada, the second-largest shipper of de minimis packages to the United States.<sup>46</sup> Customs data indicate that in 2022, more than 10 percent of Chinese imports by value now arrive as de minimis shipments, up from well under 1 percent a decade ago. In 2021, the Federal Reserve Bank of New York estimated that the U.S. Department of the Treasury loses as much as \$10 billion a year in tariffs through tariff strategies like de minimis.<sup>47</sup>

## Temu, Others Follow Shein's Model

Temu has replicated Shein's process of quickly manufacturing and shipping clothing to U.S. consumers. Temu recently sponsored two advertisements that aired during Super Bowl LVII at a cost of approximately \$14 million dollars, causing a 45 percent surge in downloads of its app and a daily active user jump of 20 percent on the day of the Super Bowl.<sup>48</sup> As of March 2023, Temu and Shein rank in the top five free apps on the Apple Store, ahead of retailers Amazon and Walmart.<sup>49</sup>

Like Shein, Temu's success raises flags about its business practices. Temu's lack of affiliation with established brands has brought concerns of product quality as well as accusations of copyright infringement. As of April 2023, Temu has received 235 complaints in the last year with the Better Business Bureau, earning a 2.1 out of 5 stars customer rating.<sup>50</sup> PDD Holdings, Temu's parent company that operates the related e-commerce platform Pinduoduo in China,\* was accused by China Labor Watch of "extreme overtime," requiring employees to work 380 hours per month.<sup>51</sup> The company faced protests online after several worker deaths in 2021.<sup>52</sup> Additionally, in April 2023, CNN reported that multiple cybersecurity teams found sophisticated malware on Pinduoduo's mobile app for Google Android devices. The malware enabled the Pinduoduo app to bypass user security permissions and access private messages, change settings, view data from other apps, and prevent uninstallation. The investigation followed Google's suspension of the app from the Google Play store in March 2023.<sup>53</sup>

Numerous other established and emerging Chinese e-commerce firms seek to penetrate the U.S. market by modeling their strategies on Shein and Temu's businesses. LightInTheBox, an established Chinese e-commerce firm listed on the New York Stock Exchange since 2013, has invested heavily in a social media strategy that mimics Shein's. With the help of a New York-based advertising agency, LightInTheBox has now partnered with more than 2,000 influencers, and the company's products reach 200 million people via influencer-posted content.<sup>54</sup> Clothing e-commerce is a surging Chinese industry. Chinese state media outlet Sixth Tone reported that there are more than ten other startup-style Chinese firms founded since 2019 emulating Shein's business model and expanding their U.S. presence, including Cider, Urbanic, ChicV, Doublefs, Cupshe, and JollyChic. Though none have the market share of Shein or Temu, all similarly offer products at comparable prices with expedited delivery times.<sup>55</sup> Their

\* PDD Holdings Inc. changed its name from Pinduoduo Inc. at an annual shareholders' meeting on February 8, 2023. PDD Holdings Inc., "Form 6-K: Report of Foreign Private Issuer Pursuant to Rule 13a-16 Or 15d-16 Under the Securities Exchange Act Of 1934," *U.S. Securities Exchange Commission*, February 9, 2023. [https://www.sec.gov/Archives/edgar/data/1737806/000110465923014742/tm235930d1\\_6k.htm](https://www.sec.gov/Archives/edgar/data/1737806/000110465923014742/tm235930d1_6k.htm).

† Sergey Toshin, director of the app security company Oversecured, found that the Pinduoduo app had exploited about 50 vulnerabilities on the Android operating system. According to CNN, Pinduoduo company insiders said the malware was intentionally developed to spy on users and competitors to boost sales. Following reports that the app included malware, the company disbanded the engineering team charged with developing malware and reportedly transferred most of them to Temu. Nectar Gan, Yong Xiong, and Juliana Liu, "I've never seen anything like this: One of China's most popular apps has the ability to spy on its users, say experts," *CNN*, April 2, 2023. <https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html>.

rapid proliferation raises concerns they will rely on controversial practices similar to those of Shein and Temu to undercut competitors and gain a foothold in the United States.

## Considerations for Congress

Given the rapid increase in the market share of Shein and other Chinese e-commerce firms in the United States, the U.S. government should be vigilant in ensuring that these firms adhere to U.S. laws and regulations and are not granted unfair advantages over U.S. firms. Congress can help safeguard U.S. interests by addressing the following gaps in U.S. policy to respond to the business models and practices of Shein and other Chinese e-commerce firms.

- *Shein and perhaps other Chinese fast fashion firms appear to be sourcing goods in violation of the Uyghur Forced Labor Prevention Act.* The investigation by Bloomberg News tracing cotton fibers to Xinjiang highlights not only the platform's likely violation of U.S. law but also that the U.S. government does not have tools to effectively screen most e-commerce shipments from China. Packages that enter the United States, including the millions that enter below the de minimis threshold, are frequently not inspected. Those that are inspected are often subject to rudimentary visual checks without the technology or screening to trace fabric origin and other violations. Without the proper staffing and technological tools, U.S. customs officials are poorly positioned to identify and cease low-cost shipments that violate U.S. laws and regulations.
- *Chinese e-commerce platforms and suppliers routinely violate U.S. IP rights laws, and the consequences they face are insufficient to deter future violations.* Several U.S. firms, from large brands to in-home studios, have singled out Chinese firms for infringing on their copyrights. This is a particular issue for independent artists who have their designs used without permission by Shein suppliers or other Chinese e-commerce platforms and suppliers, as they may not have the resources to pursue legal remedies.
- *Current customs and tariff levels disproportionately benefit Chinese e-commerce firms.* The de minimis exemption level of \$800 allows for packages shipped to the United States under that level to avoid inspection and existing tariffs. Shein and other e-commerce firms are uniquely positioned to exploit this exemption, as their products are shipped individually and nearly all fall below the de minimis threshold.

### Past Congressional and State Efforts on Chinese e-Commerce

Congress and at least one state government have already taken steps to evaluate and address the problematic practices of Chinese fast fashion firms and other Chinese e-commerce platforms.

- In February 2023, Senators Bill Cassidy (R-LA), Elizabeth Warren (D-MA), and Sheldon Whitehouse (D-RI) wrote to Shein's CEO seeking information on its alleged sourcing of Xinjiang cotton. The letter requested a response within 30 days.<sup>56</sup>
- The COMPETE Act of 2022 passed by the House in the 117th Congress included a provision to remove de minimis privileges for goods sourced from nonmarket economies with known IP violations, including China.<sup>57</sup> The bill sought to effectively close the de minimis loophole that both Shein and Temu exploit when importing goods into the United States.<sup>58</sup> After reconciliation in conference committees, however, the final CHIPS and Science Act did not include language addressing de minimis thresholds.
- At the state level, New York State's Fashion Sustainability and Social Accountability Act would more closely monitor clothing sourcing and environmental impact. The act would severely limit the market access of Shein and Temu in New York State. The act was reintroduced to the State Assembly in February 2023, with stronger provisions for legally binding environmental and labor standards in the fast fashion industry.<sup>59</sup>

## Endnotes

- <sup>1</sup> Cision PR Newswire, “Fast Fashion Global Market Report 2023,” February 17, 2023. <https://www.prnewswire.com/news-releases/fast-fashion-global-market-report-2023-301749153.html>.
- <sup>2</sup> Isabella Fish, “Inside Shein: Exclusive Interview with Chinese Fast Fashion Giant,” *Drapers*, November 2, 2022. <https://www.drapersonline.com/insight/inside-shein-exclusive-interview-with-chinese-fast-fashion-giant>; Daniel Langer, “How China Will Use AI to Master the Luxury Market,” *Jing Daily*, December 20, 2021. <https://jingdaily.com/china-luxury-artificial-intelligence-shein/>.
- <sup>3</sup> Daxue Consulting, “Shein’s Market Strategy: How the Chinese Fashion Brand Is Conquering the West,” July 6, 2022. <https://daxueconsulting.com/shein-market-strategy/>.
- <sup>4</sup> Olivia Powell, “SHEIN Fined US\$1.9mn Over Data Breach Affecting 39 Million Customers,” *Cyber Security Hub*, October 14, 2021. <https://www.cshub.com/attacks/news/shein-fined-us19mn-over-data-breach-affecting-39-million-customers>; New York State Office of the Attorney General, *Attorney General James Secures \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers’ Data*, October 12, 2022. <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop>.
- <sup>5</sup> BBC, “Shein Owner Zoetop Fined \$1.9m over Data Breach Response,” October 14, 2022. <https://www.bbc.com/news/technology-63255661>; New York State Office of the Attorney General, *Attorney General James Secures \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers’ Data*, October 12, 2022. <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop>.
- <sup>6</sup> Jerren Gan, “Here’s Why You Should Never Shop at Shein No Matter What,” *Age of Awareness*, July 14, 2021. <https://medium.com/age-of-awareness/heres-why-you-should-never-shop-at-shein-no-matter-what-8140d285cf4b>.
- <sup>7</sup> Emma Burlleigh, “After a UK Documentary Revealed Abuses, Shein Says It Will Spend \$15 Million Improving Labor Conditions,” *Observer*, December 16, 2022. <https://observer.com/2022/12/after-a-uk-documentary-revealed-abuses-shein-says-it-will-spend-15-million-improving-labor-conditions>; Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- <sup>8</sup> Bloomberg News, “Fast-Fashion Upstarts Are Using Shein’s Own Strategies against It,” November 6, 2022. <https://www.bloomberg.com/news/articles/2022-11-06/fashion-retailer-shein-s-competitors-are-copying-its-super-fast-business-model?sref=mxblZFb4>.
- <sup>9</sup> Lynn Beyrouthy, “Market Share of the Leading Fast Fashion Companies in the U.S. 2020-2022,” March 28, 2023. <https://www.statista.com/statistics/1341506/fast-fashion-market-share-us/>.
- <sup>10</sup> Janine Perri, “Shein Holds Largest U.S. Fast Fashion Market Share,” *Bloomberg Second Measure*, January 4, 2023. <https://secondmeasure.com/datapoints/fast-fashion-market-share-us-consumer-spending-data-shein-hm-zara/>.
- <sup>11</sup> MarketPlace Pulse, “Shein Is the Most-Downloaded App in the U.S.,” *Marketplace Pulse*, May 3, 2022. <https://www.marketplacepulse.com/articles/shein-is-the-most-downloaded-app-in-the-us>; Statista, “Most Downloaded Fashion & Beauty Apps in the U.S. 2022,” March 21, 2023. <https://www.statista.com/statistics/1212274/fastest-growing-fast-fashion-retailers-apps-in-the-us/>; MarketPlace Pulse, “Shein Is the Most-Downloaded App in the U.S.,” *Marketplace Pulse*, May 3, 2022. <https://www.marketplacepulse.com/articles/shein-is-the-most-downloaded-app-in-the-us>.
- <sup>12</sup> Statista, “Most Downloaded Fashion & Beauty Apps in the U.S. 2022,” March 21, 2023. <https://www.statista.com/statistics/1212274/fastest-growing-fast-fashion-retailers-apps-in-the-us/>; MarketPlace Pulse, “Shein Is the Most-Downloaded App in the U.S.,” *Marketplace Pulse*, May 3, 2022. <https://www.marketplacepulse.com/articles/shein-is-the-most-downloaded-app-in-the-us>.
- <sup>13</sup> Paul Mozur and Carolyn Zhang, “Silicon Valley Giants Confront New Walls in China,” *New York Times*, July 22, 2017. <https://www.nytimes.com/2017/07/22/technology/in-china-silicon-valley-giants-confront-new-walls.html?mcubz=0>.
- <sup>14</sup> Bloomberg News, “Amazon Is Preparing to Close a Chinese E-Commerce Store,” April 18, 2019. <https://www.bloomberg.com/news/articles/2019-04-17/amazon-is-said-to-prepare-closing-of-chinese-e-commerce-store?sref=mxblZFb4>.
- <sup>15</sup> Statista, “Social Network Ad Spending in the U.S. from 2016-2022,” January 10, 2023. <https://www.statista.com/statistics/736971/social-media-ad-spend-usa/>.
- <sup>16</sup> Sara Lebow, “Half of Younger Consumers Buy Products on Social Media,” *Insider Intelligence*, October 26, 2022. <https://www.insiderintelligence.com/content/half-of-younger-consumers-buy-products-on-social-media>.
- <sup>17</sup> Lora Jones, “Shein: The Secretive Chinese Brand Dressing Gen Z,” *BBC*, November 9, 2021. <https://www.bbc.com/news/business-59163278>.
- <sup>18</sup> Veronika Bondarenko, “TikTok Fashion Favorite Shein Considers a Big Step,” *Street*, July 15, 2022. <https://www.thestreet.com/investing/tiktok-fashion-favorite-shein-considers-a-big-step>.
- <sup>19</sup> Sarah Perez, “Shopping app Temu is using TikTok’s strategy to keep its No. 1 spot on App Store,” *Tech Crunch*, January 23, 2023. <https://techcrunch.com/2023/01/23/shopping-app-temu-is-using-tiktoks-strategy-to-keep-its-no-1-spot-on-app-store/>.
- <sup>20</sup> Shein, “Shein Influencer Program.” <https://us.shein.com/campaign/sheglaminfluencerprogram?lang=us>.
- <sup>21</sup> Temu, “Become a Temu Influencer.” <https://www temu.com/influencer-collaboration.html>.
- <sup>22</sup> Sheridan Prasso, “Shein’s Cotton Tied to Chinese Region Accused of Forced Labor,” *Bloomberg News*, November 20, 2022. <https://www.bloomberg.com/news/features/2022-11-21/shein-s-cotton-clothes-tied-to-xinjiang-china-region-accused-of-forced-labor?sref=mxblZFb4>.

- <sup>23</sup> United States Customs and Border Protection, *Uyghur Forced Labor Prevention Act*, December 23, 2021. <https://www.cbp.gov/trade/forced-labor/UFLPA>.
- <sup>24</sup> Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- <sup>25</sup> Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- <sup>26</sup> Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- <sup>27</sup> Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- <sup>28</sup> Victoria Waldersee, “EXCLUSIVE Chinese Retailer Shein Lacks Disclosures, Made False Statements about Factories,” *Reuters*, August 6, 2021. <https://www.reuters.com/business/retail-consumer/exclusive-chinese-retailer-shein-lacks-disclosures-made-false-statements-about-2021-08-06/>.
- <sup>29</sup> *Public Eye*, “Toiling Away for Shein,” November 2021. <https://stories.publiceye.ch/en/shein/>.
- <sup>30</sup> Jenny Cowley, Stephanie Matteis, and Charlsie Agro, “Experts Warn of High Levels of Chemicals in Clothes by Some Fast-Fashion Retailers,” *CBC News*, October 1, 2021. <https://www.cbc.ca/news/business/marketplace-fast-fashion-chemicals-1.6193385>.
- <sup>31</sup> Stephanie Matteis and Jenny Cowley, “Health Canada Recalls Toxic Shein Kids’ Jacket Following CBC Investigation,” *CBC*, December 9, 2021. <https://www.cbc.ca/news/canada/health-canada-recall-shein-kids-jacket-1.6279903>; Jenny Cowley, Stephanie Matteis, and Charlsie Agro, “Experts Warn of High Levels of Chemicals in Clothes by Some Fast-Fashion Retailers,” *CBC*, October 1, 2021. <https://www.cbc.ca/news/business/marketplace-fast-fashion-chemicals-1.6193385>.
- <sup>32</sup> *Greenpeace International*, “Taking the Shine off SHEIN: Hazardous Chemicals in SHEIN Products Break EU Regulations, New Report Finds,” November 23, 2022. <https://www.greenpeace.org/international/press-release/56979/taking-the-shine-off-shein-hazardous-chemicals-in-shein-products-break-eu-regulations-new-report-finds/>.
- <sup>33</sup> *World Bank*, “How Much Do Our Wardrobes Cost to the Environment?” September 23, 2019. <https://www.worldbank.org/en/news/feature/2019/09/23/costo-moda-medio-ambiente>.
- <sup>34</sup> Rachael Dottle and Jackie Gu, “The Global Glut of Clothing Is an Environmental Crisis,” *Bloomberg News*, February 23, 2022. <https://www.bloomberg.com/graphics/2022-fashion-industry-environmental-impact/?sref=mxblZFb4>.
- <sup>35</sup> Good on You, “Shein,” March, 2023. <https://directory.goodonyou.eco/brand/shein>.
- <sup>36</sup> Dan Strumpf, “China’s Fast-Fashion Giant Shein Faces Dozens of Lawsuits Alleging Design Theft,” *Wall Street Journal*, July 3, 2022. <https://www.wsj.com/articles/chinas-fast-fashion-giant-shein-faces-dozens-of-lawsuits-alleging-design-theft-11656840601>.
- <sup>37</sup> *The Fashion Law*, “Shein Owner Zoetop Claims Dr. Martens Trademarks Are Generic,” October 26, 2021. <https://www.thefashionlaw.com/in-response-to-airwair-lawsuit-shein-owner-zoetop-claims-dr-martens-trademarks-are-generic/>.
- <sup>38</sup> Dan Strumpf, “China’s Fast-Fashion Giant Shein Faces Dozens of Lawsuits Alleging Design Theft,” *Wall Street Journal*, July 3, 2022. <https://www.wsj.com/articles/chinas-fast-fashion-giant-shein-faces-dozens-of-lawsuits-alleging-design-theft-11656840601>.
- <sup>39</sup> Lora Jones, “Shein: The Secretive Chinese Brand Dressing Gen Z,” *BBC*, November 9, 2021. <https://www.bbc.com/news/business-59163278>.
- <sup>40</sup> Kenneth Rapoza, “How a U.S. Trade Loophole Called ‘De Minimis’ Is China’s ‘Free Trade Deal,’” *Forbes*, February 19, 2023. <https://www.forbes.com/sites/kenrapoza/2023/02/19/how-a-us-trade-loophole-called-de-minimis-is-chinas-free-trade-deal/?sh=508503b64c9b>; Bloomberg News, “How Trump’s Trade War Built Shein, China’s First Global Fashion Giant,” June 14, 2021. <https://www.bloomberg.com/news/articles/2021-06-14/online-fashion-giant-shein-emerged-from-china-thanks-to-donald-trump-s-trade-war?sref=mxblZFb4>.
- <sup>41</sup> David Morse, “The Pleasure Island of Shein,” *Coalition for a Prosperous America*, February 9, 2023. <https://prosperousamerica.org/the-pleasure-island-of-shein/>.
- <sup>42</sup> FTI Consulting, “Outcome of ‘De Minimis’ Will Have Major Effects on eCommerce Importations and the U.S. FTZ Program,” May 16, 2022. <https://www.fticonsulting.com/insights/articles/outcome-de-minimis-effects-ecommerce-importations-us-ftz>.
- <sup>43</sup> Alavara, “De Minimis Value: A Minimum Value Defined by a Country Required to Apply Customs Duty and Tax Rates on Imported Goods.” <https://www.alavara.com/us/en/learn/cross-border-resources/de-minimis-threshold-table.html>.
- <sup>44</sup> U.S. Customs and Border Protection, *Trade Statistics*. <https://www.cbp.gov/newsroom/stats/trade>.
- <sup>45</sup> Kenneth Rapoza, “How a U.S. Trade Loophole Called ‘De Minimis’ Is China’s ‘Free Trade Deal,’” *Forbes*, February 19, 2023. <https://www.forbes.com/sites/kenrapoza/2023/02/19/how-a-us-trade-loophole-called-de-minimis-is-chinas-free-trade-deal/?sh=5fa293544c9b>.
- <sup>46</sup> United States Customs and Border Protection, “SECTION 321 DE MINIMIS SHIPMENTS FISCAL YEAR 2018 to 2021 STATISTICS,” *United States Customs and Border Protection*, October, 2022. [www.cbp.gov/sites/default/files/assets/documents/2022-Oct/FY2018-2021\\_De%20Minimis%20Statistics%20update.pdf](http://www.cbp.gov/sites/default/files/assets/documents/2022-Oct/FY2018-2021_De%20Minimis%20Statistics%20update.pdf).
- <sup>47</sup> Josh Zumbrun, “The \$67 Billion Tariff Dodge That’s Undermining U.S. Trade Policy,” *Wall Street Journal*, April 25, 2022. <https://www.wsj.com/articles/the-67-billion-tariff-dodge-thats-undermining-u-s-trade-policy-di-minimis-rule-customs-tourists-11650897161>.
- <sup>48</sup> Vidhi Choudhary, “After a Successful Super Bowl Ad, Temu’s Growth Is Outpacing Rivals Like Target,” *Modern Retail*, February 21, 2023. <https://www.modernretail.co/technology/after-a-successful-super-bowl-ad-temus-growth-is-outpacing-rivals-like-target/>.
- <sup>49</sup> Apple, “Top Charts.” <https://apps.apple.com/us/charts/iphone/top-free-apps/36>.
- <sup>50</sup> Better Business Bureau, “Temu.” <https://www.bbb.org/us/ma/boston/profile/online-shopping/temucom-0021-553943>.
- <sup>51</sup> Wilfred Chan, “Chinese Behemoth Pinduoduo to Take on Amazon in US – with Even Worse Labor Practices,” *Guardian*, August 25, 2022. <https://www.theguardian.com/technology/2022/aug/25/pinduoduo-us-labor-practices-worker-conditions>.

- <sup>52</sup> Vivian Wang, “Worker Deaths Put Big Tech in China under Scrutiny,” *New York Times*, February 1, 2021. <https://www.nytimes.com/2021/02/01/business/china-technology-worker-deaths.html>.
- <sup>53</sup> CNN, “‘I’ve never seen anything like this:’ One of China’s most popular apps has the ability to spy on its users, say experts,” *CNN*, April 2, 2023. <https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html>.
- <sup>54</sup> The Setters, “LightInTheBox.” <https://thesetters.agency/cases/case2/lightinthebox>.
- <sup>55</sup> China Service Association, “2021-2022 年中国服装电子商务发展报告” (“2021-2022 China’s Clothing e-Commerce Development Report”), *China Garment Association*, May 23, 2022. Translation. [https://www.sixthtone.com/news/1009020/being-shein-chinese-retailers-eye-the-global-fast-fashion-market](http://webcache.googleusercontent.com/search?q=cache:oCFzsQ0k_gsJ:www.cnga.org.cn/html/shouye/remenzixun/2022/0523/54504.html%3F1653324274&cd=1&hl=en&ct=clnk&gl=us; Jiang Yaling, “Becoming Shein: Chinese Retailers Eye the Global Fast-Fashion Market,” <i>Sixth Tone</i>, November 19, 2021. <a href=).
- <sup>56</sup> Office of Bill Cassidy, “Cassidy, Warren, Whitehouse Press SHEIN On Connection to Chinese Slave Labor Supply Chains,” *Office of Bill Cassidy*, February 9, 2023. <https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-warren-whitehouse-press-shein-on-connection-to-chinese-slave-labor-supply-chains>.
- <sup>57</sup> Braumiller Law Group, “Understanding the America Competes Act of 2022 - What Upcoming Major Changes to International Trade Law Should You Know About?” *Braumiller Law Group*. <https://www.lexology.com/library/detail.aspx?g=cdf14301-3330-496f-96af-f17d9e2e25a0>.
- <sup>58</sup> Congressman Earl Blumenauer, “THE IMPORT SECURITY AND FAIRNESS ACT,” *Congressman Earl Blumenauer*, [blumenauer.house.gov/sites/evo-subsites/blumenauer-evo.house.gov/files/One%20Pager%20-%20Import%20Security%20and%20Fairness%20Act.pdf](https://blumenauer.house.gov/sites/evo-subsites/blumenauer-evo.house.gov/files/One%20Pager%20-%20Import%20Security%20and%20Fairness%20Act.pdf).
- <sup>59</sup> Kaley Roshitch, “Albany Bound: ‘Fashion Act’ Supporters Hope to Stir Renewed Support,” *WWD*, March 8, 2023, <https://wwd.com/sustainability/business/new-york-fashion-act-supporters-albany-sustainability-bills-1235576182/>; Nicole Grenfield, “New York Is Exposing the Fashion Industry for What It Is: a Climate Nightmare,” *NRDC*, February 13, 2023. <https://www.nrdc.org/stories/new-york-exposing-fashion-industry-what-it-climate-nightmare>.





Post

Settings

Tom Cotton @SenTomCotton

TikTok exposes Americans' data to the Chinese government, exposes children to harmful content, and is a source of propaganda.

We should ban it in the U.S. or force it to be sold.



1:16 PM · Mar 10, 2024 · 54.2K Views

222 Reposts 43 Quotes 827 Likes 15 Bookmarks



New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Relevant people

Tom Cotton @SenTomCotton U.S. Senator proudly serving the state of Arkansas.

Something went wrong. Try reloading.

Retry

Terms of Service Privacy Policy Cookie Policy Accessibility Ads info More ... © 2024 X Corp.

Don't miss what's happening People on X are the first to know.

Log in Sign up

APP-553

JA 348

# *House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App*

The legislation received wide bipartisan support, with both Republicans and Democrats showing an eagerness to appear tough on China.



**By Sapna Maheshwari, David McCabe and Annie Karni**

March 13, 2024

The House on Wednesday passed a bill with broad bipartisan support that would force TikTok's Chinese owner to either sell the hugely popular video app or have it banned in the United States.

The move escalates a showdown between Beijing and Washington over the control of a wide range of technologies that could affect national security, free speech and the social media industry.

Republican leaders fast-tracked the bill through the House with limited debate, and it passed on a lopsided vote of 352 to 65, reflecting widespread backing for legislation that would take direct aim at China in an election year.

The action came despite TikTok's efforts to mobilize its 170 million U.S. users against the measure, and amid the Biden administration's push to persuade lawmakers that Chinese ownership of the platform poses grave national security risks to the United States, including the ability to meddle in elections.

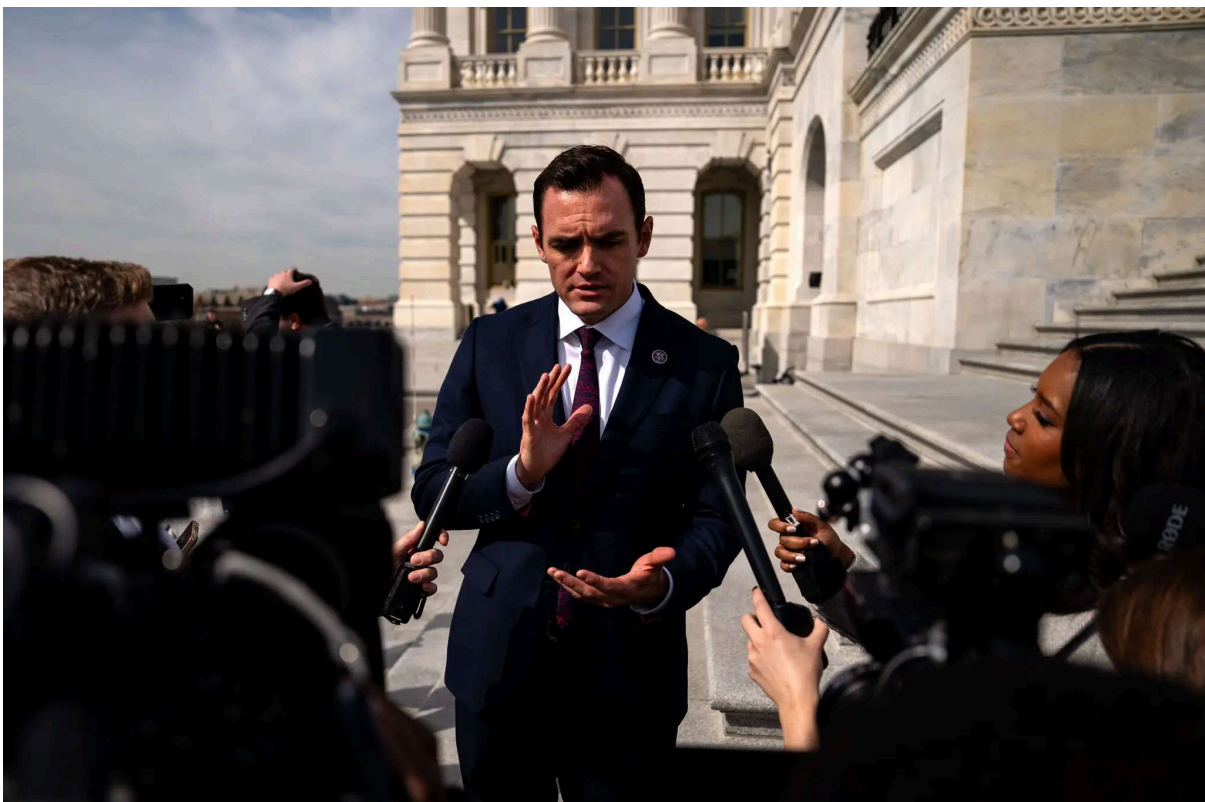
The result was a bipartisan coalition behind the measure that included Republicans, who defied former President Donald J. Trump in supporting it, and Democrats, who also fell in line behind a bill that President Biden has said he would sign.

The bill faces a difficult road to passage in the Senate, where Senator Chuck Schumer, Democrat of New York and the majority leader, has been noncommittal about bringing it to the floor for a vote and where some lawmakers have vowed to fight it. And even if it passes the Senate and becomes law, it is likely to face legal challenges.

But Wednesday's vote was the first time a measure that could widely ban TikTok for consumers was approved by a full chamber of Congress. The app has been under threat since 2020, with lawmakers increasingly arguing that Beijing's relationship with TikTok's parent company, ByteDance, raises national security risks. The bill is aimed at getting ByteDance to sell TikTok to non-Chinese owners within six months. The president would sign off on the sale if it resolved national security concerns. If that sale did not happen, the app would be banned.

Representative Mike Gallagher, the Wisconsin Republican who is among the lawmakers leading the bill, said on the floor before the vote that it "forces TikTok to break up with the Chinese Communist Party."

"This is a common-sense measure to protect our national security," he said.



Representative Mike Gallagher, the Wisconsin Republican who is among the lawmakers behind the bill. Kent Nishimura for The New York Times

Alex Haurek, a spokesman for TikTok, said in a statement that the House “process was secret and the bill was jammed through for one reason: It’s a ban.”

“We are hopeful that the Senate will consider the facts, listen to their constituents, and realize the impact on the economy — seven million small businesses — and the 170 million Americans who use our service,” he added.

On Wednesday, before the House vote, Beijing condemned the push by U.S. lawmakers and rejected the notion that TikTok was a danger to the United States. At a daily press briefing, Wang Wenbin, a spokesman for China’s foreign ministry, accused Washington of “resorting to hegemonic moves when one could not succeed in fair competition.”

If the bill were to become law, it would likely deepen a cold war between the United States and China over the control of many important technologies, including solar panels, electric vehicles and semiconductors.

Mr. Biden has announced limitations on how U.S. financial firms can invest in Chinese companies and restricted the sale of Americans’ sensitive data like location and health information to data brokers that could sell it to China. Platforms like Facebook and YouTube are blocked in China, and Beijing said last year that it would oppose a sale of TikTok.

TikTok has said that it has gone to great lengths to protect U.S. user data and provide third-party oversight of the platform, and that no government can influence the company’s recommendation model. It has also said there is no proof that Beijing has used TikTok to obtain U.S. user data or to influence Americans’ views, two of the concerns lawmakers have cited.

In an unusually aggressive move for a technology company, TikTok urged users to call their representatives last week to protest the bill, saying, “This legislation has a predetermined outcome: a total ban of TikTok in the United States.”

TikTok has spent more than \$1 billion on an extensive plan known as Project Texas that aims to handle sensitive U.S. user data separately from the rest of the company's operations. That plan has for several years been under review by a panel known as the Committee on Foreign Investment in the United States, or CFIUS.

Two of the lawmakers behind the bill, Mr. Gallagher and Raja Krishnamoorthi, an Illinois Democrat, said last week that lawmakers were acting because CFIUS “hasn't solved the problem.”

It's very unusual for a bill to garner broad bipartisan support but at the same time divide both parties. President Biden has said he would sign the bill into law, but top House leaders like Representative Katherine Clark of Massachusetts, the No. 2 Democrat in the House, voted against the bill. Mr. Trump said he opposed the bill, but many of his most stalwart allies in the House, like Representative Elise Stefanik of New York, the No. 4 Republican in the House, voted for it.

The vote came down to something of a free-for-all, with unusual alliances in support of and opposed to the bill. Representative Nancy Pelosi, Democrat of California and the former house speaker, sat in the chamber nodding along with hard-right Republicans like Representative Dan Crenshaw, Republican of Texas, as they outlined their support for the bill. At one point, she got up and crossed over to the Republican side of the aisle to confer with Representative Chip Roy, a hard-right Republican of Texas, who had vocally supported the bill on the floor.

Several Republicans and Democrats expressed their opposition to the bill based on free speech concerns and TikTok's popularity in the United States. Some legal experts have said that if the bill were to become law, it would probably face First Amendment scrutiny in the courts.

Representative Maxwell Frost, a Democrat of Florida, said on Tuesday that “not only am I no, but I'm a hell no.” He said the legislation was an infringement of First Amendment rights. “I hear from students all the time that get their information,

the truth of what has happened in this country, from content creators on TikTok.” He said he was concerned about Americans’ data, but “this bill does not fix that problem.”



Representative Maxwell Frost at a news conference with TikTok creators on Capitol Hill on Tuesday. Haiyun Jiang for The New York Times

There wasn't any legislation last year in the aftermath of a fiery hearing with Shou Chew, TikTok's chief executive, despite bipartisan support to regulate the app. But concern among lawmakers has grown even more in recent months, with many of them saying that TikTok's content recommendations could be used for misinformation, a concern that has escalated in the United States since the Israel-Hamas war began.

“It was a lot of things in the interim, including Oct. 7, including the fact that the Osama bin Laden ‘Letter to America’ went viral on TikTok and the platform continued to show dramatic differences in content relative to other social media platforms,” Mr. Krishnamoorthi said in an interview.

There's also a chance that even if the bill is signed and survives court challenges, it could crumble under a new administration. Mr. Trump, who tried to ban TikTok or force its sale in 2020, publicly reversed his position on the app over the past week. In a television appearance on Monday, Mr. Trump said that the app was a national security threat, but that banning it would help Facebook, a platform the former president criticized.

“There are a lot of young kids on TikTok who will go crazy without it,” he said.

Mr. Trump's administration had threatened to remove TikTok from American app stores if ByteDance did not sell its share in the app. ByteDance even seemed ready to sell a stake in the app to Walmart and Oracle, where executives were close to Mr. Trump.

That plan went awry in federal court. Multiple judges stopped Mr. Trump's proposed ban from taking effect.

Mr. Biden's administration has tried turning to a legislative solution. The White House provided “technical assistance” to Mr. Gallagher and Mr. Krishnamoorthi as they wrote their bill, Karine Jean-Pierre, the White House press secretary, said at a briefing last week. When the bill was introduced, a National Security Council spokesman quickly called the legislation “an important and welcome step to address” the threat of technology that imperils Americans' sensitive data.

The administration has repeatedly sent national security officials to Capitol Hill to privately make the case for the legislation and offer dire warnings on the risks of TikTok's current ownership. The White House briefed lawmakers before the 50 to 0 committee vote last week that advanced the bill to the full House.

On Tuesday, officials from the Federal Bureau of Investigation, the Office of the Director of National Intelligence and the Justice Department spoke with lawmakers in a classified briefing about national security concerns tied to TikTok.

Mr. Gallagher and Mr. Krishnamoorthi had previously sponsored a bill aimed at banning TikTok. The latest bill has been viewed as something of a last stand against the company for Mr. Gallagher, who recently said he would not run for a

fifth term because “the framers intended citizens to serve in Congress for a season and then return to their private lives.”

**Sapna Maheshwari** reports on TikTok, technology and emerging media companies. She has been a business reporter for more than a decade. Contact her at [sapna@nytimes.com](mailto:sapna@nytimes.com). More about Sapna Maheshwari

**David McCabe** covers tech policy. He joined The Times from Axios in 2019. More about David McCabe

**Annie Karni** is a congressional correspondent for The Times. She writes features and profiles, with a recent focus on House Republican leadership. More about Annie Karni



CQ Newsmaker Transcripts

Mar. 14, 2024

Mar. 14, 2024 Revised Final

---

## Sen. Warner Interviewed on Fox News

### LIST OF SPEAKERS

NEIL CAVUTO, FOX NEWS ANCHOR:

All right, you know what happened in the House.

In an overwhelming vote that was bipartisan, the move was, TikTok cannot be what it is right now, controlled by China, and that means ByteDance, the parent company of China, must unload it, divest it, as they say on Wall Street.

But it isn't getting the same reaction in the United States Senate. Again, Chuck Schumer has not even detailed if or even when the Senate will take it up.

Senator Mark Warner joins us right now. He is the Senate Intelligence Committee chairman.

Senator, good to have you.

Do you think the Senate should take up this issue?

SEN. MARK WARNER (D-VA):

Absolutely.

Neil, I have been on your show many, many times talking about the national security threat that is posed by having a platform that 170

million Americans use on average 90 minutes a day. China is collecting this data about lots of Americans.

And what is even more problematic for me is, the genius of TikTok is, it knows what you like before you know what you like. And a lot of young people get all their news. They could switch the algorithm a little bit and suddenly all the TikTok videos will be promoting that Taiwan ought to be part of China, or that Putin's right...

CAVUTO:  
Right.

WARNER:  
... on getting Ukraine. And I think...

CAVUTO:  
No, all these examples you raised, you obviously eloquently put the key arguments here.

But it doesn't look like Chuck Schumer either agrees or sees the need to do something right now.

WARNER:  
Well...

CAVUTO:  
Now, that could change. Is it your understanding that it will and the Senate will take up the matter?

WARNER:

Well, listen, Neil, I know Senate never moves quickly on anything.

But my friends in the House, that was a huge vote, 352 votes. It was just yesterday. I think, Schumer, I have had preliminary conversations. Chair Cantwell on the Commerce Committee is going to have views. There may be things that need to be slightly altered or amended.

But I think anyone who cares about -- we have plenty of divisions in our country.

CAVUTO:

Yes.

WARNER:

We ought to be able to argue amongst ourselves, left and right, Republican, Democrat. We don't need the Chinese Communist Party dominating or influencing.

(CROSSTALK)

CAVUTO:

So, the sheer size of that vote, the sheer size of that vote in the House would maybe -- has maybe changed the thinking in the Senate, as far as you...

WARNER:

I think so.

CAVUTO:

OK.

WARNER:

I would say so.

(CROSSTALK)

CAVUTO:

So let me ask you about that then, Senator.

One other idea that's been bandied about, if ByteDance were to go ahead and divest itself of **TikTok**, no sure thing, that **TikTok** would essentially be for sale one way or the other. A lot of American names have come into play here. Oracle's name comes up, Microsoft, Meta, of course, the Facebook parent.

Do you have any concerns with any of those names?

WARNER:

Well, I have concerns about too much concentration, if this was acquired by another social media company.

And, frankly, that's all of our preference. If you like **TikTok**, if you're a social influencer on that, you want to be, and you make your living that way, that's great with me. It just ought to be a company that's not controlled by China.

So I was really glad to see Donald Trump's Treasury Secretary Steve Mnuchin put out word today that he was trying to put together a group of investors that could potentially buy this application. I think that he'd be great. He was one of the guys that first educated me on this issue.

And I know I have said this. I don't say this often, even on FOX, but, on TikTok, Donald Trump was right years ago in saying it was a national security threat. Now, he's changed his tune a little bit now.

CAVUTO:

Yes.

WARNER:

But his initial indication on this as a national security threat was right. And I think it would be great if a group of investors were to buy this.

So the service could still be extended. People could still get to see all the crazy and fun videos, but, ultimately, it would be with American or European or somebody other than Chinese ownership.

CAVUTO:

You know, it doesn't quite cut black and white, right, Senator? I mean, you mentioned Donald Trump changing his mind on this, that maybe we don't get rid of it for the time being or push to get rid of it.

But it is a hot political issue, or could be, right? Because 170 million Americans use this.

WARNER:

Yes.

CAVUTO:

Lopsidedly, they're young, and they don't want it to go away.

WARNER:

Well...

CAVUTO:

And that they might get ticked off and take it out on politicians who do push to have it go away.

WARNER:

I hear it. And that's why I say, let's not have it go away. Let's just not have the Communist Party of China pulling its strings.

I think...

CAVUTO:

But what do you -- how do you react when young people say, they don't care, Senator?

WARNER:

But...

CAVUTO:

They figure that everyone spies on them when they're online. It's not forgivable, don't get me wrong, but that they don't draw the distinction China doing it versus an American company doing it, as you're still being spied on.

How do you react to that? How do you talk to them?

WARNER:

Well, I would react a couple of ways.

One, that funny or inappropriate video two, five years from now, if somebody's trying to blackmail you from the Chinese spy services, I don't think you're going to want that to happen. And even if they don't care about the propaganda purposes, we would never let the Chinese Communist Party buy FOX News or MSNBC.

The idea that they have this propaganda channel that can affect Americans' views, again, we got plenty to fight about amongst ourselves.

CAVUTO:

Yes.

WARNER:

Let's not turn the reins over.

And one of the reasons that I think that something will happen is that we have done nothing on social media for years. I mean, the fact that we don't even have any kids online safety, again, broad bipartisan support for that, if we can't at least start with something that is this pervasive, controlled by an adversary of the United States, then all the things that folks think about Washington are true.

But I got a lot of hope; 352 people in the House, I didn't think you would get 352 House members to agree on anything.

CAVUTO:

No, you're quite right about that. You're quite right about it.

Let me ask you. You were mentioning the possibility how would we react to the Chinese where -- you first mentioned FOX News and

Home > ... > Secretary Antony J. Blinken At McCain Institute's 2...

## Secretary Antony J. Blinken At McCain Institute's 2024 Sedona Forum Keynote Conversation with Senator Mitt Romney

### REMARKS

ANTHONY J. BLINKEN, SECRETARY OF STATE  
SEDONA, ARIZONA

MAY 3, 2024

**SENATOR ROMNEY:** I don't know who gets to go off first, but I'm going to do that, because I get to ask the questions. I'm not the questioner, usually. Usually I'm the person trying to give answers, all right? Have you ever watched Mr. Roger's Neighborhood? There's a little train and there's the little king, and he – the king is always right – “Right as usual, King Friday.” My kids say, “Right as usual, King Romney.” I mean, because I'm – (laughter) – I'm always out there with the answers.

So I – tonight I'm supposed to ask the questions, which I will do. But I want to begin by saying thank you to Cindy McCain for hosting us and bringing this extraordinary group together. Thank you to the Navalny family and for your beautiful words – extraordinary. Thank you so very much for your inspiration. It is touching and powerful. Thank you to the McCain Institute. Thank you to David Axelrod. I have mixed emotions about David Axelrod. (Laughter.)

I appreciate the Secretary of State and his leadership very much. And we're fortunate to have a Secretary of State who's a thoughtful, perceptive, intellectually curious, devoted person; dedicated, determined, indefatigable, who has traveled the world time and time again – not a person of bombast, but a person who listens and is soft-spoken. We are very fortunate to have a man of the kind of quality, experience, and character as our current Secretary of State, Secretary Antony Blinken. Thank you. (Applause.)

So because I'm not noted for my questions – and frankly, my answers aren't much better – (laughter) – but I'm going to ask a few questions, but if there's a little time, I might turn to you to ask, if there are questions. I'm going to just sort of go topic area by topic area. I'm going to start with the Secretary's most recent trip to the Middle East and then turn to Ukraine, and then finally to China. And so if there's someone who has a question on one of those topics, or – I'll take a breath, and you can – and please ask questions that are interesting to you, but also, you might think, to the entire audience. (Laughter.)

First, I'm going to say up top, with regards to the trip to the Middle East, give us the lowdown, give us the rundown. What is happening there? What's happening among the Israeli people? What are – what is Bibi Netanyahu thinking? What's happening with Hamas? What kind of a deal has been put on the table? What's – what is – the people and the leadership in Qatar – see, I can get all my questions out. (Laughter.) I mean, give us a full lay of the land, and then we can sort of probe areas of interest.

**SECRETARY BLINKEN:** Mitt, thank you. And before trying to tackle that multi-part question – (laughter) – actually, it sounds like —

**SENATOR ROMNEY:** It's – it's just the lay of the land.

**SECRETARY BLINKEN:** It sounds like the reporters in my pool, who manage to get in five questions for one.

First, let me say how wonderful it is to be here and to be with a truly remarkable group of people. I think there's a common denominator in this room, and it's epitomized by John McCain, it's epitomized by Mitt Romney, but everyone in this room is for an engaged America. Everyone in this room believes that our engagement, our leadership matters, makes a difference. And that commitment is more important than it's ever been. That's what I'm seeing and feeling around the world.

Now, it may be that years from now people come back here and look at this group, and it's the La Brea Tar Pits of internationalists and institutionalists. (Laughter.) But we're fighting to make sure that's not the case, and no one has fought harder than the gentleman sitting to my right.

Now, Mitt, I was going to say thank you for reading the lines that I wrote – (laughter) – appreciate that. But I think you all know – the country all knows – Mitt Romney is a man of extraordinary principle, married to extraordinary pragmatism. It's a rare combination, and I've gotten to see that up close these last few years since you've been in the Senate. But for me, it's an honor to share the stage with you. So thank you. (Applause.)

**SENATOR ROMNEY:** Thank you.

**SECRETARY BLINKEN:** And to the entire McCain family, starting with Cindy – following in the footsteps of John McCain – there too I have gotten to work with Cindy these last few years. You are doing what is maybe the greatest calling anyone could have, which is trying to make sure that parents can put food on the table for their kids. And when it comes down to it, nothing matters more than that. So to you, to the entire family that remains so engaged, it's wonderful to be here and to share this evening with you.



Now, I have to tell you – and maybe the Middle East is actually a – it's a perfect segue to the Middle East. But let me just say quickly, before we were coming out here, we were listening, Dasha, we were listening to you, and the senator and I had the same reaction: Let's go in the other direction, because we don't want to follow Dasha. (Laughter.) Thank you for your extraordinary profile in dignity and in courage. And I can only imagine how proud your dad would be of you. (Applause.)

So when I'm asked how it's going, and the Middle East is usually the first thing I'm asked about, I actually tend to quote John McCain. John McCain used to say, "It's always darkest before it goes completely black." (Laughter.) So – and I thank you, Cindy, for letting me borrow that.

But now to get serious for a minute, so in this moment, the best thing that can happen would be for the agreement that's on the table that's being considered by Hamas – to have a ceasefire, the release of hostages, the possibility of really surging humanitarian assistance to people who so desperately need it – that's what we're focused on. And as I was talking to various colleagues this morning – and I see one of my closest colleagues, John Finer, the deputy national security advisor, here – we await a response from Hamas. We await to see whether, in effect, they can take yes for an answer on the ceasefire and release of hostages. And the reality in this moment is the only thing standing between the people of Gaza and a ceasefire is Hamas. So we look to see what they will do.

In the meantime, even as we're doing that, we are working every single day, the President's working every single day, to make sure that we are doing what we can so that the people in Gaza who are caught in a crossfire of Hamas's making get the help, the assistance, the support they need. And we're doing that with partners like the World Food Program; and of course, we're working with many other governments, we're working with Israel.

I was just there, as you said, and I got to see firsthand some of the progress that's been made in recent weeks in actually getting assistance to people who need it. Progress is real; it's still not enough. And we are trying to make sure that in everything we do, we're supporting those efforts.

If you step back, I think we've seen a few things in the last few weeks – some incredibly promising, others incredibly daunting. And to start with the daunting, we now have the Israelis and Palestinians, two absolutely traumatized societies, and when this conflict ends, building back from that trauma is going to be an extraordinary task.

We also see in all directions – and I think we're seeing this not only in the region, we're seeing it around the world; to some extent we're seeing it in our own country – maybe the biggest poison that we have to fight constantly, and that is dehumanization, the inability to see the humanity in the other. And when that happens, hearts get hardened, and everything becomes so much more difficult.

So the other great task that I think we're going to have when we get through this is to build back that sense of common humanity. And I hope we can do that amongst ourselves as well. But there's also some promise. There's promise in that one of the things we've been working on for a long time, with the President's leadership over many months, is seeking to normalize relations between Saudi Arabia and Israel. And for Israel, this would be the realization of something that it's sought from day one of its existence: normal relations with other countries in the region.

This is something we were working on before October 7th. In fact, I was due to go to Israel and Saudi Arabia on October 10th to work on this, and in particular to work on the Palestinian piece of the puzzle, because for us, for the Saudis, if we're able to move forward on normalization, it has to include also moving forward on the aspirations of the Palestinian people.

So I think there's an equation that you can see, a different path that countries in the region can be on and really want to be on, which is a path of integration, a path where Israel's relations with its neighbors are normalized; a path where Israel's security is actually looked out for, including by its neighbors; a path where Palestinians achieve their political rights; and a path in which the biggest threat to Israel, to most of the countries in the region, and a threat that we share, Iran, is actually isolated.

Now, whether we can move from the moment that we're in to actually start to travel down that path, that's going to be a big challenge. But you can see it, and it's something that the President is determined to try to pursue if we have the opportunity to do it.

One other thing on this. We saw something related that was quite extraordinary about two weeks ago. Iran engaged in an unprecedented attack on Israel, the first direct attack from Iran to Israel. And some people said, well, it was designed so it wouldn't do much damage, carefully calibrated. Nothing of the sort. More than 300 projectiles launched at Israel, including more than a hundred ballistic missiles. John and I were in the Situation Room watching this unfold.

It's because Israel had very effective defenses – but also because the President, the United States, managed to rally on short notice a collection of countries to help – that damage was not done. And that also shows something in embryonic form: the possibilities that Israel has for, again, being integrated, a regional security architecture that can actually, I think, keep the peace effectively for years to come.

So that's where we want to go. But getting from here to there, of course, requires that the war in Gaza come to an end. And right now, the quickest path to that happening would be through this ceasefire and hostage deal.

**SENATOR ROMNEY:** I think a number of folks, myself included, have wondered why Hamas has not agreed to other proposals with regards to a ceasefire. What are we misunderstanding? What is their calculation? What are they – why are they hesitating? This – I mean, we read about what's being proposed. It sounds like a no-brainer. But they must have a different calculation. What is going through their head? What – I mean, they want to be just martyrs? Is that – I mean, what is it that they hope to carry out, and why have they not just jumped on this, saying, oh, yeah, this is fantastic?

**SECRETARY BLINKEN:** One of the challenges we have, of course, is that the leaders of Hamas that we're indirectly engaged with through the Qataris, through the Egyptians, are of course living outside of Gaza, living in Qatar or living in Türkiye, other places, and the ultimate decision makers are the folks who are actually in Gaza itself with whom none of us have direct contact. So trying to understand what they're thinking is a challenge. Now, we have some sense of it, but it's not – it's far from perfect. And there are different theories about what's actually motivating their decisions in this time. It's something we – we're constantly trying to get at.

But I can't give you a definitive answer, and I think we'll see, depending on what they actually do in this moment, whether in fact the Palestinian people whom they purport to represent – if that's actually true; because if it is true, then taking the ceasefire should be a no-brainer, as you said. But maybe something else is going on, and we'll have a better picture of that in the coming days.

**SENATOR ROMNEY:** Tell us about Bibi Netanyahu and what his – what his position of power is, how he's seen among the Israeli people, what the level of commitment is in Israel for them to go into Rafah, to continue this effort. Where is he? If this – well, I'm not – I'm going to take the if out. I was going to go back to the ceasefire. But what's his political posture now in Israel?

**SECRETARY BLINKEN:** Well, I think, as everyone knows, this is a complicated government. It's a balancing act when you have a coalition. And if you're just looking at the politics of it, that's something that he has to factor in.

But here's what I'd say generally about this. Irrespective of what you think of the prime minister, the government, what's important to understand is that much of what he's doing is not simply a reflection of his politics or his policies; it's actually a reflection of where a large majority of Israelis are in this moment. And I think it's important to understand that if we're really going to be able to meet this challenge. That's at least my observation.

I've now been there seven times since October 7th, and you get a chance to get a feel for what's going on in the society itself. And as I said at the start, you have a traumatized society, just as you have traumatized Palestinians. And breaking through that trauma in real time is an extraordinary challenge. But it's I think very important that we, as the United States, as Israel's friend, try to share what we think is not only in our interest but also what's in their interest. And when it comes to Rafah – Mitt, you mentioned that a moment ago – look, our position is clear. The President's been clear on this. Absent a credible plan to genuinely protect civilians who are in harm's way – and keep in mind there are now 1.4 million or so people in Rafah, many of them displaced from the north – absent such a plan, we can't support a major military operation going into Rafah because the damage it would do is beyond what's acceptable.

So we haven't seen such a plan yet, but right now, as I said, the focus is intensely on seeing if we can't get this agreement because that would be a way of, I think, moving things in a different direction.

**SENATOR ROMNEY:** You may not want to answer this question, but that is – the President sort of dipped his toe into the criticism of Israel and the way they've conducted the war so far, saying we're not entirely happy with how this has been carried out. What would our administration have done differently? What is our specific criticism, and what guidance will that provide for what they do going forward?

**SECRETARY BLINKEN:** Well, let's start with the – in a sense, the obvious that seems to have been forgotten, or almost erased from the conversation, which is October 7th itself. And it's extraordinary how quickly the world moved on from that.

It's also extraordinary the extent to which Hamas isn't even part of the conversation. And I think that's worth a moment of reflection, too. And so we've said from the start, and the President has been committed from the start, to the proposition that Israel not only has a right to defend itself, not only has a right to try to make sure October 7th never happens again, it has an obligation. And so that's something that we have supported from day one.

But we've also said – also from day one – how it does it matters. And here, the damage that's been done to so many innocent children, women, and men – again, in this crossfire of Hamas's making – has to be something that we focus on, as it has been from day one, trying to make sure that the assistance gets to those who need it, trying to make sure that civilians are protected to the greatest extent possible.

Now, everyone here knows that this is a – almost a unique challenge because when you have an enemy, a terrorist group like Hamas that embeds itself with the civilian population in ways that we really haven't seen before, and that is hiding in and under mosques, schools, apartment buildings, it's an incredibly tall order. But even so, even so, I think where we've been pushing our friends – again, from the very start – is to do as much as possible, and to do more, to look out for civilians, and to make sure that those who need the help get it.

**SENATOR ROMNEY:** Why has the PR been so awful? I know that's not your area of expertise, but you have to have some thoughts on that, which is, I mean, as you've said, why has Hamas disappeared in terms of public perception? An offer is on the table to have a ceasefire, and yet the world is screaming about Israel. It's like, why are they not screaming about Hamas? Accept the ceasefire and bring home the hostages. Instead, it's all the other way around. I mean, typically the Israelis are good at PR. What's happened here? How have they – how have they/ and we/ been so ineffective at communicating the realities there and our point of view?

**SECRETARY BLINKEN:** Look, I mean, there are two things. One is that, look, there is an inescapable reality, and that is the inescapable reality of people who have and continue to suffer grievously in Gaza. And that's real and we have to – have to – be focused on that and attentive to that.

At the same time, how this narrative has evolved, yeah, it's a great question. I don't have a good answer to that. One can speculate about what some of the causes might be. I don't know. I can tell you this – and we were talking about this a little bit over dinner with Cindy. I think in my time in Washington, which is a little bit over 30 years, the single biggest change has been in the information environment. And when I started out in the early 1990s, everyone did the same thing. You woke up in the morning, you opened the door of your apartment or your house, you picked up a hard copy of *The New York Times*, *The Washington Post*, *The Wall Street Journal*. And then if you had a television in your office, you turned it on at 6:30 or 7 o'clock and watched the national network news.

Now, of course, we are on an intravenous feed of information with new impulses, inputs every millisecond. And of course, the way this has played out on social media has dominated the narrative. And you have a social media ecosystem environment in which context, history, facts get lost, and the emotion, the impact of images dominates. And we can't – we can't discount that, but I think it also has a very, very, very challenging effect on the narrative.

**SENATOR ROMNEY:** A small parenthetical point, which is some wonder why there was such overwhelming support for us to shut down potentially TikTok or other entities of that nature. If you look at the postings on TikTok and the number of mentions of Palestinians relative to other social media sites, it's overwhelmingly so among TikTok broadcasts. So I'd note that's of real interest, and the President will get the chance to make action in that regard.

The President had also spoken about our commitment to a two-state solution, and a number of people have said to me that's impossible. And Bibi Netanyahu has basically said that's impossible. Is it possible to have a two-state solution? What kind of – I mean, I know that's far from where we are right now. It's like a whole different realm. But is that essential to, if you will, beginning normalization relations with Saudi Arabia and with others to say, hey, here's a vision, here's some steps we might get to? Is it possible, and what would that look like?

**SECRETARY BLINKEN:** So for me and the President, the answer is yes. And you can say that's – especially in this moment – naïve, impossible. But I think that it is an imperative. And let me put it this way. First, we were talking about normalization with Saudi Arabia. I've sat with MBS multiple times, the crown prince, and he's made clear that he wants to pursue normalization and he'd like to do it as soon as possible – if we can conclude the agreements that we're trying to reach between the United States and Saudi Arabia. But then two requirements: one, calm in Gaza; two, a credible pathway to a Palestinian state. This is what people in the region need to see if they're going to fully get behind normalized relations between the remaining Arab countries and Israel. And it's also the right thing for the Palestinians. So there's that.

But the other, I think, more fundamental question is this. You've got 5 million Palestinians living between the West Bank and Gaza. You've got about 7 million Jews. The Palestinians aren't going anywhere; the Jews aren't going anywhere. There has to be an accommodation. Now, I think that some believe that the status quo that prevailed before October 7th – fine, let's live that way. And that worked brilliantly until it failed catastrophically.

So at some point, I believe there has to be a step back. And everyone's going to have to ask themselves questions about what do we want the future to be. And the future that I talked about a few minutes ago, where Israel finally realizes what it has sought from day one – to be accepted in the region, to be part of the neighborhood – that's achievable. It's there, but it also requires a resolution to the Palestinian question. And I believe that there can be a Palestinian state with the necessary security guarantees for Israel. And to some extent, I think you have Israelis who would like to get to real separation. Well, that is one way to do it. And then who knows what happens in the following years.

But of course, as we say this, we are absolutely committed to Israel's security. And Israel cannot and will not accept a Hamastan coming together next door. But I'm convinced that there are ways to put the Palestinians on a pathway to a state that demonstrate that the state will not be what Israelis might fear, and I think can lead to a much better future than we have.

Look, everyone in this room knows there's a long story here. We were talking about TikTok. Not a story you hear on TikTok. You had – to oversimplify, after the creation of the state of Israel you had decades of basically Arab rejection. That went away with Egypt and Jordan making peace, and others following. Then you had some decades, in effect, of Palestinian rejection, because deals were put on the table – Camp David, Ehud Olmert, others – that would have given Palestinians 95, 96, 97 percent of what they sought, but they were not able to get to yes. But I think the last decade or so has been one in which maybe Israelis became comfortable with that status quo. And as I say, I just don't think it's sustainable.

**SENATOR ROMNEY:** Yeah. Yeah. Anyone else, topic? Israel, Middle East? Yes, sir.

**QUESTION:** (Inaudible.)

**SENATOR ROMNEY:** You've got to be real loud. And I'm going to repeat it, but it's got to be short, too.

**QUESTION:** All right, it's very short. You talked about Israel and Palestine, Saudi Arabia being such a key U.S. ally there. What do you see with China, Taiwan, India, Japan kind of doing the same (inaudible)? What efforts (inaudible)? What are the complications that you're running into trying to overcome the China threat and the Russian threat to European allies?

**SECRETARY BLINKEN:** Maybe that's a great segue. Did we need a segue?

**SENATOR ROMNEY:** There you go, go ahead. Yeah, please.

**SECRETARY BLINKEN:** All right. Well, just a few things to say here. First, with China, just before we were in the Middle East we were in China. And about a little less than a year ago, I took a trip at a time when we had been very disengaged. And I think that one of the things that President Biden believes is that we have an obligation to try to manage this relationship responsibly. We're in an intense competition with China, and of course, for Americans there's nothing wrong with competition as long as it's fair. Hopefully it actually brings out the best in us. But it is a real competition.

But we also have a profound interest in making sure that competition doesn't veer into conflict, and that actually starts with engagement. And so we really began a process of re-engagement with our eyes wide open, and a number of my colleagues followed. And then, of course, most important, President Biden and President Xi met at the end of the year in San Francisco on the margins of the APEC meeting.

And what we've tried to do, first and foremost, is to re-establish regular dialogue at all levels. One of the most important pieces of this was re-establishing military-to-military communications, because the quickest way to get into an unintended conflict is not to have those conversations happen. That's been fully restored. We look for areas where we might actually cooperate where it happens to be in our mutual interest to do that – and I'll come back to this in a second because we found a couple. But mostly, it's so important because you want to be able to be extremely clear, extremely direct, extremely explicit about your differences and your intentions. And we have a world of differences, but it's better to be talking about them directly than it is to remain disengaged.

**JA 366**

**APP-596**

**SCHEDULED FOR ORAL ARGUMENT IN SEPTEMBER 2024**

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

TIKTOK INC.,

and

BYTEDANCE LTD.,

*Petitioners,*

v.

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

*Respondent.*

No. 24-1113

**DECLARATION OF RANDAL S. MILCH**

**JUNE 17, 2024**

**TABLE OF CONTENTS**

I. Qualifications.....1

II. Assignment and Summary of Opinions.....3

III. Opinions.....6

    A. Divestitures of highly integrated assets are complex and time-consuming processes.....6

    B. Certain divestitures are more complex than others.....10

    C. A “qualified divestiture” of TikTok’s U.S. application would be highly complex.....12

    D. Market examples show that complex divestitures are time-consuming processes .....18

        1. My experience with Verizon’s divestitures illustrates the time-consuming and complex nature of divesting highly integrated assets ..... 18

        2. Other high-value divestitures in the TMT sector illustrate the length and complexity of divesting highly integrated assets ..... 23

    E. A “qualified divestiture” of TikTok’s U.S. application is not operationally feasible within the timeline required by the Act.....42

## I. QUALIFICATIONS

1. I am a Professor of Practice at New York University (“NYU”) School of Law, where I have taught courses in cybersecurity, hacking, regulation, and corporate governance since 2018. I am a Faculty Director of the NYU Master of Science in Cybersecurity Risk & Strategy Program. I also serve as the co-chair of the NYU Center for Cybersecurity. In these roles, I have developed, and I direct, an academic program that seeks to bridge the gaps between technical and non-technical cybersecurity professionals. Since 2015, I have also been a Distinguished Fellow at the Reiss Center for Law and Security at NYU School of Law. I was previously a lecturer in law at Columbia Business School, where I co-taught a course on public policy and business strategy.

2. Prior to my work at NYU, I was employed for 21 years at Verizon Communications Inc. (“Verizon”) and its corporate predecessor Bell Atlantic.<sup>1</sup> From 2008 to 2014, I served as Verizon’s Executive Vice President, Public Policy, and General Counsel. In that role I was responsible for, among other matters, all state, federal, and international regulatory, public policy, and national security issues at Verizon. Beginning in 2008, I was the senior officer at Verizon holding a Top Secret/Sensitive Compartmented Information security clearance. I received that clearance in 2006, when I began serving as the Senior Vice President and General Counsel of Verizon Business, Verizon’s global enterprise business. From 2000 to 2005, I served as the Senior Vice President and General Counsel of Verizon Telecom, where I

---

<sup>1</sup> For the remainder of my declaration, I include all of Verizon’s corporate predecessors (including General Telephone & Electronics Corporation, or “GTE”) in the term “Verizon.” Verizon was created by the merger of Bell Atlantic with GTE in 2000. Both parties brought with them their long-held legacy wireline assets. *See* “Bell Atlantic and GTE Complete Their Merger and Become Verizon Communications,” Verizon News Archives, June 30, 2000, <https://www.verizon.com/about/news/press-releases/bell-atlantic-and-gte-complete-their-merger-and-become-verizon-communications>.

was responsible for, among other matters, all state regulatory and public policy issues affecting Verizon's landline businesses in the United States. In the foregoing roles at Verizon, I was involved in the divestiture of numerous assets, as I will describe later in this declaration.

3. From 1997 to 2000, I served as Vice President and Associate General Counsel of Bell Atlantic, where my responsibilities included implementation of all aspects of the 1996 Telecommunications Act, including its competition provisions. This role included developing and litigating the case before the New York Public Service Commission that resulted in Verizon New York being the first Bell company allowed to enter the long distance and enterprise markets. The principal issue in that case concerned the development of software operation support systems to interconnect competitors' ordering systems with Bell Atlantic-New York's operations systems. I was, as a result, deeply involved in the requirements for, and testing of, complex software. I joined a Bell Atlantic subsidiary, Bell Atlantic-Maryland, in 1993 as a regulatory attorney.

4. I received my bachelor's degree in American History from Yale University in 1980, and my Juris Doctor (J.D.) from NYU School of Law in 1985. I held a judicial clerkship for the Honorable Clement F. Haynsworth, Jr., in the United States Court of Appeals for the Fourth Circuit. A current copy of my curriculum vitae is included as **Appendix A** to this declaration. I have previously testified under oath before various Committees of Congress, including on national security issues. A list of my unclassified testimony is included in my curriculum vitae.

5. In preparing this declaration, I received research support from individuals at Analysis Group, Inc., a consulting firm, working under my direction and guidance.

6. The sources I have relied upon are cited throughout this declaration. Should additional relevant documents or information be made available to me, I may adjust or supplement my opinions as appropriate.

## II. ASSIGNMENT AND SUMMARY OF OPINIONS

7. I have been retained by Counsel for TikTok Inc. and ByteDance Ltd. (together, “Petitioners”)<sup>2</sup> to evaluate whether a potential divestiture of the integrated global TikTok platform’s (“TikTok”) U.S. application is feasible from an operational perspective within the timeframe and under the restrictions set out in the Protecting Americans from Foreign Adversary Controlled Applications Act (the “Act”), signed on April 24, 2024.

8. On its face, the Act appears to present Petitioners with a choice: (a) sell TikTok’s U.S. application on terms set out in the Act, or (b) be banned from operating TikTok in the United States. The ban occurs by default under the Act by making it unlawful in the United States to: (1) provide internet hosting services to Petitioners; and (2) distribute mobile applications operated by Petitioners after January 19, 2025 (or, if the President permits, after April 19, 2025).<sup>3</sup> Thus, the TikTok application will be banned within the United States after these deadlines unless Petitioners have made a “qualified divestiture” of TikTok’s U.S. application on or before the deadlines.<sup>4</sup>

---

<sup>2</sup> “ByteDance Ltd.” is a corporate entity incorporated in the Cayman Islands. “TikTok Inc.” is a corporate entity incorporated in the United States. “TikTok” is an online application that includes the TikTok mobile application and TikTok through a web browser.

<sup>3</sup> The Act, Section 2(a)(1).

<sup>4</sup> The prohibition defined by the Act takes effect on January 19, 2025, which is 270 days after the enactment of the Act (on April 24, 2024). The President may extend this deadline by three months (to April 19, 2025) if a path to a qualified divestiture has been identified or significant progress has been made. The Act, Section 2(a)(2)-(3).



9. As I discuss below, it is my opinion that the divestiture option is entirely illusory and that the Act in fact imposes a ban on TikTok’s U.S. application after the relevant deadlines.<sup>5</sup> Because a “qualified divestiture” under the Act is one in which the TikTok application operated in the United States cannot have “any operational relationship” with Petitioners,<sup>6</sup> it is my opinion that a “qualified divestiture” of TikTok’s U.S. application would not be operationally feasible by January (or even April) 2025. I base my opinion on my: (1) review of relevant literature, (2) review of information about TikTok, (3) experience with complex divestitures of highly integrated assets, and (4) evaluation of publicly available information on divestitures in the technology, media, and telecommunications (“TMT”) sector.

10. As I explain below, divestitures of highly integrated assets are complex and time-consuming processes. Sellers and buyers of divested assets must undertake two efforts. The first effort can be thought of as comprising “corporate” steps, such as negotiations between buyer and seller, the signing of a definitive agreement between the parties, seeking regulatory approval for the deal, and the closing of the transaction. The second effort (which may partially overlap with the first) involves “operational” steps, which generally entail planning for and executing the

---

<sup>5</sup> I have been instructed by Counsel to assume that the asset to be divested in any qualified divestiture would be the TikTok U.S. application, as opposed to discrete assets of the TikTok business. For this reason, I have not analyzed the timelines associated with theoretical options of a buyer acquiring only parts of TikTok’s U.S. application or buying the application with the intention to engage in asset stripping, such as by liquidating any real estate assets or monetizing solely its user list data. I understand that Counsel’s interpretation is consistent with the language of the Act, which contemplates the qualified divestiture of the TikTok “application,” as well as statements from congressional sponsors. Rep. Krishnamoorthi, for example, has stated: “This particular bill ensures that ByteDance divests itself of the vast majority of the ownership of TikTok. Our intention is for TikTok to continue to operate [...]” “House Debate on H.R. 7521, H1163-1171,” Congressional Record — House, March 13, 2024, <https://www.congress.gov/118/crec/2024/03/13/170/45/CREC-2024-03-13-pt1-PgH1163-2.pdf>.

<sup>6</sup> The Act “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.” The Act, Section 2(g)(6)(B).

carve-out of the financial, personnel, physical, and software assets that will be divested with the business.

11. These operational steps, particularly in complex divestitures of highly integrated assets, take a considerable length of time.<sup>7</sup> In each example of complex divestitures of highly integrated assets that I evaluated, the operational timeline was much longer than the 270 (or 360) days afforded to Petitioners under the Act. Because the Act precludes the buyer from having “any operational relationship” with Petitioners as of the statutory deadline, all operational steps must be completed before the applicable deadline for the divestiture to satisfy the definition of a “qualified divestiture.”<sup>8</sup>

12. The complexity of a divestiture—and thus the amount of time it takes to achieve, all else equal—increases if there is a high level of integration (*i.e.*, the extent to which complex systems are shared) between the divested asset and the rest of the seller’s company. The information I reviewed regarding a potential divestiture of TikTok’s U.S. application suggests that achieving a “qualified divestiture” would be highly complex given, among other potential factors, the high level of integration between TikTok’s U.S. application and the global TikTok application. As I describe in **Section III.C**, this remains the case notwithstanding the technological and governance protections on which Petitioners have been working.<sup>9</sup>

13. My experience with facilitating complex divestitures at Verizon shows that divesting highly integrated assets to the point where the seller has no operational relationship takes much longer than the time afforded to Petitioners in the Act (in the Verizon examples,

---

<sup>7</sup> As I describe below in **Section III.A**, the corporate timeline can also take hundreds of days. I have made the conservative assumption in my declaration that Petitioners could achieve a corporate timeline of zero days.

<sup>8</sup> The Act, Section 2(g)(6)(B).

<sup>9</sup> See paragraph 29 for a discussion of “Project Texas.”

approximately twice as long as the time afforded to Petitioners). My personal experience is corroborated by my evaluation of the operational timelines associated with the divestitures of certain highly integrated assets in the TMT sector.

14. For the above reasons and as further explained below, it is my opinion that achieving a “qualified divestiture” of TikTok’s U.S. application is operationally infeasible within the timeframe and under the restrictions set out in the Act. Therefore, the Act offers no real alternative to Petitioners and instead amounts to a *de facto* ban on the TikTok application in the United States starting on January (or April) 19, 2025.

### III. OPINIONS

#### A. Divestitures of highly integrated assets are complex and time-consuming processes

15. Divestitures—the partial or full disposal of a company’s business unit, division, subsidiary, product line, or other assets—are complex undertakings.<sup>10</sup> As I described above, in addition to “corporate” steps, companies must also undertake “operational” steps. As shown in **Figure 1**, when divesting integrated assets, the operational timeline begins when the parties start discussing the mechanics of the transition (which may occur before or after signing the deal) and

---

<sup>10</sup> Joy, Joseph (2018), *Divestitures and Spin-Offs: Lessons Learned in the Trenches of the World’s Largest M&A Deals* (1st ed. 2018), Springer US (“Joy 2018”), p. 457 (“Divestitures are complex endeavors”). *See also* Joshi, Varun and Sharma, Saurav (2013), Chapter 1 Introduction to the IT Aspects of Mergers, Acquisitions, and Divestitures, In J. M. Roehl-Anderson (Ed.), *M&A Information Technology Best Practices* (pp. 1-22), Wiley (“Joshi 2013”), p. 14 (“Identifying and carving out the pieces in a divestiture can be a complex and time-consuming process”). I include within my definition of “divestitures” spinoffs (*i.e.*, “a type of divestiture in which the divested unit becomes an independent company instead of being sold to a third party”) and splitoffs (*i.e.*, divestitures similar to spinoffs where the shareholders “relinquish their shares of stock in the parent company in order to receive shares of the subsidiary company”). Lessambo, Felix (2021), Chapter 12 Corporate Divestitures and Carve-Outs, In *U.S. Mergers and Acquisitions* (pp. 159-170), Springer, p. 163; CFI Team, “Spin-Off,” CFI, <https://corporatefinanceinstitute.com/resources/valuation/spin-off-and-split-off/>.

ends when the new owner operates the divested assets without the seller’s assistance (which may occur on or after the deal’s closing).

**Figure 1 - Divestiture Timelines<sup>11</sup>**



16. To this end, prior to closing, buyers often contract with the seller to assist with the post-closing operation of the divested asset, such as by providing access to existing software and associated expertise through Transition Services Agreements (“TSAs”) or other similar arrangements.<sup>12</sup> TSAs and similar agreements provide the buyer with access to technology or other support after closing to maintain business continuity.<sup>13</sup> However, TSAs and similar agreements are far from ideal for either the buyer or the seller.<sup>14</sup> For example, by relying on the seller to provide key technology services to the buyer, the buyer loses direct control over its newly acquired systems and can face increased security risks. Similarly, the seller is often

<sup>11</sup> Adapted from Joy 2018, p. 186, based on my professional experience.

<sup>12</sup> Joy 2018, pp. 374, 451-453.

<sup>13</sup> Joy 2018, pp. 374, 451-453. *See also* Joshi 2013, p. 14 (“Depending on the strategy [from financial close to full separation/exit], it may be beneficial for certain services to be covered under a [TSA]. A TSA is a legal agreement, separate from the separation and purchase agreement, in which the buyer agrees to pay the seller for certain services to support the divested business for a defined period of time. TSAs are most often used in carve-outs where the buyer lacks the necessary information technology capabilities or capacity to support the business on its own. [...] TSAs are also often necessary when the deal closes faster than the buyer’s organization can respond.”).

<sup>14</sup> Joy 2018, pp. 34, 433.

obliged by the service agreement to direct its resources to provide services to the buyer, which diverts resources away from the seller's core business.<sup>15</sup> Therefore, both parties typically seek to keep the length of transition services as short as possible.

17. Importantly, because the Act precludes a buyer of TikTok's U.S. application from having "any operational relationship" with Petitioners after January (or April) 2025,<sup>16</sup> the Act effectively limits the entire timeline (corporate and operational) to 270 (or perhaps 360) days.<sup>17</sup>

18. As my analysis below shows, the corporate timeline—which primarily affords the parties the time to analyze and negotiate the allocation of deal risks between them<sup>18</sup>—can take hundreds of days.<sup>19</sup> However, because the parties can control certain basic elements of the corporate timeline, the parties may decide to accelerate this timeline (by, for instance, foregoing some risk mitigation steps, such as due diligence).<sup>20</sup> In contrast, the parties typically cannot

---

<sup>15</sup> Joy 2018, pp. 34, 433.

<sup>16</sup> The Act, Section 2(g)(6)(B).

<sup>17</sup> I note that, from the day of submitting my declaration on June 20, 2024, Petitioners have only 214 days left until January 19, 2025; and they have only 304 days left until April 19, 2025. Nevertheless, throughout my declaration, to be conservative, I use 270 and 360 days as the operative figures.

<sup>18</sup> Jacob Orosz, "The M&A Purchase Agreement | An Overview," Morgan & Westfield, <https://morganandwestfield.com/knowledge/purchase-agreement/> ("The purchase agreement can also be seen as a tool for allocating risk between buyer and seller.").

<sup>19</sup> The corporate steps include, among other things: identifying the divestment approach (*e.g.*, through a spin-off or a carve-out); identifying the buyer; defining the divestiture strategy; addressing legal, financial, human resources, and information technology considerations; signing; and closing. These steps generally take a considerable amount of time. *See, for example*: Richard D. Harroch, David A. Lipkin, and Richard V. Smith, "What You Need To Know About Mergers & Acquisitions: 12 Key Considerations When Selling Your Company," *Forbes*, August 27, 2018, <https://www.forbes.com/sites/allbusiness/2018/08/27/mergers-and-acquisitions-key-considerations-when-selling-your-company/?sh=2ef58cd84102>; Jens Kengelbach, Alexander Roos, and Georg Keienburg, "Maximizing Value: Choose the Right Exit Route," BCG, September 22, 2014, <https://www.bcg.com/publications/2014/mergers-acquisitions-divestitures-maximizing-value>; Joy 2018, pp. 26-28.

<sup>20</sup> In some cases, divestitures also require the approval of regulatory authorities, such as the Federal Trade Commission or the Federal Communications Commission. A detailed study of recent transactions shows that seeking regulatory approval can delay the transaction by "three to six months [...], but more complicated deals often take twice as long, up to two years." (*See* Suzanne Kumar, Adam Haller, and Dale Stafford, "Regulation and M&A: How Scrutiny Raises the Bar for Acquirers," Bain & Company, January 30, 2024,

meaningfully accelerate the operational timeline. This is because—due to the need to continue operating the divested assets—operational steps cannot be accomplished in less time than the time required for employees to plan and execute the “physical separation of the [...] IT infrastructure, applications, and data, from the divesting company,” which “often includes separating data and processes within legacy IT systems that were not designed or built to enable future decoupling.”<sup>21</sup> The common utilization of TSAs, which as noted are not ideal for either party, demonstrates that operational timelines cannot be meaningfully compressed despite economic incentives to do so.

19. Because the parties can control certain basic elements of the corporate timeline, I have made the conservative assumption in my declaration that Petitioners could achieve a corporate timeline of zero days. However, even assuming Petitioners could have instantaneously negotiated a divestiture agreement on the day the Act was signed into law, they still could not achieve a qualified divestiture within the timeline allowed by the Act: as I show below, the

---

<https://www.bain.com/insights/regulation-m-and-a-report-2024/>.) Regulatory delays are typically not in the parties’ control. Because regulatory delays are part of the corporate timeline, and my analysis focuses on operational timelines, my analysis does not include the time required to achieve regulatory approvals.

<sup>21</sup> Philip W. Yetton et al., “How IT Carve-Out Project Complexity Influences Divestor Performance in M&As,” *European Journal of Information Systems*, Vol. 32, No. 6, 2023, pp. 962-988 (“Yetton 2023”), at p. 965. *See also* Yetton 2023, at p. 964 (“[T]he timeframe in the contract is frequently too tight to execute the required IT carve-out. In that case, Operational Day 1 represents an operationally viable *intermediate IT-state* [emphasis in original] in which the provision of IT services by the divestor is formally enabled by TSAs. [...] TSAs are attractive because they make an earlier Operational Day 1 possible and provide reliable IT support until Physical IT Separation.”); at p. 976 (“[W]ith increasing project complexity, the transfer of IT assets to the acquirer is incompatible with the set Operational Day 1 [...]. The time constraint contingent on satisfying Operational Day 1 readiness is particularly problematic in the context of IT carve-out projects because the time constraint on the project is not based on an estimate of the time required for the project but set by market expectations for the acquirer to realise [sic] acquisition benefits.”). *See also* Joshi 2013, p. 10 (“[Day 1] requirements should be highly focused on keeping the business running, removing uncertainty for stakeholders, complying with regulatory requirements, and delivering the Day 1 must-haves”); Kin, Blair (2013), Chapter 21 Planning for Business Process Changes Impacting Information Technology, In J. M. Roehl-Anderson (Ed.), *M&A Information Technology Best Practices* (pp. 376-377), Wiley, pp. 376-377 (“[t]he IT staff will need to have a full understanding of what functions will remain in use so the proper changes can be made. This effort is time-consuming for the IT staff that is already engaged in changes to other complicated post-merger integrations.”).

operational timelines alone of divestitures with similar levels of integration as TikTok took longer than 360 days (let alone 270 days).

**B. Certain divestitures are more complex than others**

20. While I would consider any divestiture a complex undertaking, there is a range of complexity, and certain divestitures are more complex than others. Academic and industry participants have identified specific characteristics that affect the complexity of a divestiture. For example, the Divestiture Complexity Assessment (“DCA”) Framework considers, among other factors, the following two key factors when gauging the complexity of a planned divestiture.<sup>22</sup>

- a) **The level of integration**, *i.e.*, the extent to which the divested asset and the rest of the seller share information technology (“IT”) systems and applications, and the ease with which the seller can separate these systems and applications.<sup>23</sup> The greater the level of integration, the more complex the divestiture because the “IT function [is] the most complex function to separate.”<sup>24</sup>
- b) **Post-divestiture support from the seller**, *i.e.*, whether the seller will provide support to the divested asset in the form of TSAs or other arrangements after the

---

<sup>22</sup> Joy 2018, pp. 17-18.

<sup>23</sup> The DCA framework uses the term “comingling” [sic] for integration. Joy 2018, pp. 17-18.

<sup>24</sup> Joy 2018, p. 12. *See also* Yetton 2023, at p. 965 (“IT carve-out projects are frequently complex, accounting for more than 50% of the overall carve-out cost”); Joshi 2013, p. 14 (“Identifying and carving out the pieces in a divestiture can be a complex and time-consuming process, particularly when the affected people, processes, and systems are deeply integrated within the seller’s business, or when services and infrastructure are shared across multiple business units”); p. 5 (“IT-related activities are generally the largest cost items in a merger or divestiture”); p. 20 (“IT integrations or separations are generally complex, resource-intensive initiatives that need to be closely aligned with the overall business integration effort”).

divestiture.<sup>25</sup> Divestiture processes become more complex when the seller is less able (or willing) to support the divested asset post-divestiture, because if that is the case, the entirety of the operational effort must occur before closing.<sup>26</sup>

21. The importance of these factors in gauging the expected complexity of a divestiture is consistent with my professional experience in facilitating complex divestitures of highly integrated assets. While other factors certainly play a role in the complexity of a divestiture (such as creating a separate financial framework for the divested asset, and dealing with employee matters), based on my experience the above two factors are particularly relevant in determining complexity.

22. As I describe in the following sections, I have evaluated historical divestitures and the “qualified divestiture” the Act requires from Petitioners along the following dimensions.

- a. To capture the extent of “integration” and the ease with which the divested asset could be separated from the rest of the seller, I evaluated the following:
  - i. Whether the divested asset can be separated from the rest of the seller based solely on product market.<sup>27</sup> If that is the case, isolating the divested

---

<sup>25</sup> The DCA framework uses the term “Health of the seller company” for post-divestiture support from the seller. *See* Joy 2018, p. 18 (“How is the health of the seller company? Will it be able to provide support to the buyer in form of TSAs post-divestiture? Is there any dependency on the seller company post-divestiture?”).

<sup>26</sup> *See, e.g.*, Joshi 2013, p. 14 (“TSAs are most often used in carve-outs where the buyer lacks the necessary information technology capabilities or capacity to support the business on its own. [...] TSAs are also often necessary when the deal closes faster than the buyer’s organization can respond.”).

<sup>27</sup> A divested asset can be defined based solely on product market if geographic considerations are not necessary to define the asset. For example, if a company divests its software business in Canada while continuing to operate the same business in the United States, this divestiture is not defined based solely on product market. However, if a company divests its entire software business (regardless of geography), while retaining its hardware business, this divestiture is defined based solely on product market.



asset is simpler than if the divestiture involves separating one or more products into multiple pieces based on geographic market.

- ii. Whether the seller acquired the divested asset within ten years of the evaluated divestiture. This fact suggests a more limited level of “integration” of the divested asset with the rest of the seller than if the seller had developed the divested asset organically or if the seller had acquired it more than ten years before the evaluated divestiture.<sup>28</sup>

- b. I also evaluated whether the deal included a TSA or a similar agreement that indicates ongoing technical support from the seller after the deal closed.<sup>29</sup>

**C. A “qualified divestiture” of TikTok’s U.S. application would be highly complex**

23. While the details of a potential “qualified divestiture” of TikTok’s U.S. application are currently unknowable, the information that I have reviewed indicates that any “qualified divestiture” of the U.S. application would be highly complex.

24. First, TikTok’s U.S. application and global application are highly integrated. TikTok’s U.S. application offers the same product as TikTok’s global application—that is, the asset to be divested would be defined only by a geographic market, even though the asset is part

---

<sup>28</sup> I use the ten-year benchmark as a proxy for an expected level of integration between an acquired asset and the acquirer. Based on my experience, all else equal, companies have an economic incentive to integrate operations over time. As I describe below, my conclusions would not change even if the threshold were different. First, none of the divestitures I evaluated in **Section III.D** had indicia of being non-complex based on the ten-year acquisition criterion alone. Second, none of the divestitures I evaluated in **Section III.D** took fewer than 270 days.

<sup>29</sup> As I discuss in **Section III.D**, public companies and companies in regulated industries frequently face obligations to disclose details regarding their divestitures, providing transparency into otherwise concealed divestiture steps.

of a global platform and product. Further, TikTok’s U.S. application is an organic part of TikTok’s global platform; Petitioners did not acquire “TikTok U.S.”<sup>30</sup> Indeed, the Draft National Security Agreement (“NSA”) defines the “TikTok U.S. Application” as “all versions of the TikTok Global App provided to, or accessible by, TikTok U.S. Users,”<sup>31</sup> suggesting that the “TikTok U.S. Application” is indistinguishable from the “TikTok Global App.”

25. Second, the global TikTok application itself is highly integrated with ByteDance.<sup>32,33</sup> The Harvard Business Review attributes ByteDance’s success in part to its “shared-service platform” model. ByteDance has centralized many technology, operating, and business functions into “shared-service platforms” that can be flexibly deployed to handle many

---

<sup>30</sup> ByteDance’s 2017 acquisition of Musical.ly is irrelevant for this evaluation because divesting TikTok’s U.S. application would be far different than unwinding the Musical.ly transaction. Although ByteDance initially ran Musical.ly as an “independent platform” (“China’s ByteDance Buying Lip-Sync App Musical.ly for Up to \$1 Billion,” Reuters, November 10, 2017, <https://www.reuters.com/article/idUSKBN1DA0BQ/>), before relaunching TikTok in the United States in August 2018, ByteDance “abandoned the Musical.ly code base and technology, including Musical.ly’s recommendation engine, operation system, user growth, and marketing tools.” (Petition, *TikTok Inc. et al v. CFIUS*, No. 20-1444, November 10, 2020, pp. 9-10.) ByteDance integrated Musical.ly’s “user base, some music licensing agreements and other copyright agreements” with the “technology platform [...] developed by ByteDance before the Musical.ly acquisition had even occurred.” (See Petition, *TikTok Inc. et al v. CFIUS*, No. 20-1444, November 10, 2020, pp. 9-10. See also Rebecca Fannin, “The Strategy Behind TikTok’s Global Rise,” Harvard Business Review, September 13, 2019, <https://hbr.org/2019/09/the-strategy-behind-tiktoks-global-rise>.) As a result, the current TikTok app in the United States has only the barest attributes of the Musical.ly app from 2017 and there is essentially no Musical.ly app to divest.

<sup>31</sup> Draft National Security Agreement by and Among: (i) ByteDance Ltd., (ii) TikTok Ltd., (iii) TikTok Inc., and (iv) CFIUS Monitoring Agencies, on behalf of the CFIUS, August 23, 2022.

<sup>32</sup> Kane Wu and Julie Zhu, “Exclusive: ByteDance Prefers TikTok Shutdown in US if Legal Options Fail, Sources Say,” Reuters, April 26, 2024, <https://www.reuters.com/technology/bytedance-prefers-tiktok-shutdown-us-if-legal-options-fail-sources-say-2024-04-25/> (“The algorithms TikTok relies on for its operations are deemed core to ByteDance’s overall operations. [...] TikTok shares the same core algorithms with ByteDance domestic apps like short video platform Douyin.”). By ByteDance I mean to refer to the general corporate group, as opposed to any particular corporate entity.

<sup>33</sup> Counsel instructed me to evaluate whether a “qualified divestiture” of TikTok’s U.S. application, as opposed to TikTok’s global application, would be operationally feasible within the timeframe and under the restrictions set out in the Act. That noted, my opinions set out in this declaration would not change if I were to evaluate a “qualified divestiture” of TikTok’s global application. This is because, as I describe in this section, such a divestiture would remain a complicated geographic splitting of a highly integrated product: in this case, the integration of the global TikTok application with ByteDance.

tasks across products—including core engineering tasks.<sup>34</sup> The Harvard Business Review’s description of the “shared-service platform” across ByteDance’s products is consistent with Petitioners’ submission to the Committee on Foreign Investment in the United States (“CFIUS”) in August 2021, explaining that the TikTok application (and ByteDance’s other applications) are composed of thousands of “microservices,”<sup>35</sup> whereby “small, self-contained teams” can separately develop the software for each service.<sup>36</sup> This approach allows product engineering teams to rapidly leverage technologies across products, in effect integrating the software underlying ByteDance’s various apps.<sup>37,38</sup>

26. Third, as I described above, the Act precludes Petitioners from having “any operational relationship” with the buyer after January (or April) 2025.<sup>39</sup> Therefore, the Act effectively prohibits TSAs or other post-divestiture support arrangements. This restriction means that the entire timeline (corporate and operational), including all planning, development, and transition implementation must be completed by the deadline, rendering the divestiture more complex.

---

<sup>34</sup> Roger Chen and Rui Ma, “How ByteDance Became the World’s Most Valuable Startup,” Harvard Business Review, February 24, 2022, <https://hbr.org/2022/02/how-bytedance-became-the-worlds-most-valuable-startup> (“In some cases, product teams customize existing technologies that have already been developed by the SSP [or Shared-Service Platform]. Algorithms are a case in point. Product teams at ByteDance work with SSP algorithm engineers to fine-tune their enormously powerful recommendation engines. [...] As expected, because so many capabilities have been centralized into this large SSP, the actual product teams tend to be small and focused”).

<sup>35</sup> CFIUS Questions for ByteDance/TikTok, August 26, 2021, p. 13.

<sup>36</sup> “What Are Microservices?,” AWS, <https://aws.amazon.com/microservices/>.

<sup>37</sup> Roger Chen and Rui Ma, “How ByteDance Became the World’s Most Valuable Startup,” Harvard Business Review, February 24, 2022, <https://hbr.org/2022/02/how-bytedance-became-the-worlds-most-valuable-startup>.

<sup>38</sup> Although ByteDance has provided information to CFIUS regarding the changes that it has made to its software development process since 2021 as part of Project Texas, these changes do not alter my opinion regarding the high level of integration and complexity of a “qualified divestiture” of TikTok’s U.S. application. *See* paragraph 29 for additional information.

<sup>39</sup> The Act, Section 2(g)(6)(B).

27. Fourth, according to Petitioners, Chinese export control laws would forbid the divestment of certain elements of TikTok’s integrated software, including in particular its recommendation engine.<sup>40</sup> According to information provided by Petitioners to CFIUS, as of October 2022, TikTok’s global application consisted of roughly 2 billion lines of code.<sup>41</sup> According to public reports, this length of code is on the same scale as Google was in 2015.<sup>42</sup> Similarly, according to Petitioners, as of August 2021, there were approximately 4,000 software engineers working on the global TikTok application (with only about 800 of them located in the United States).<sup>43</sup> The total number of 4,000 engineers is on the same scale as Uber.<sup>44</sup> To the extent that—as the result of an export ban—the buyer would need to recreate elements of TikTok’s software before January (or April) 19, 2025, TikTok’s large scale further adds to the complexity of the divestiture. Based on the Act, after the deadline, Petitioners would not be allowed to provide the buyer breathing room while the buyer recreates this infrastructure (*e.g.*, the buyer would not be allowed to run TikTok on the old code while the new code was being created).<sup>45</sup>

---

<sup>40</sup> See Letter from Michael E. Leiter, et al., to David Newman (Principal Deputy Assistant Attorney General for National Security), April 1, 2024, pp. 1-2.

<sup>41</sup> “TikTok Source Code Update,” October 24, 2022.

<sup>42</sup> Cade Metz, “Google Is 2 Billion Lines of Code—And It’s All in One Place,” WIRED, September 16, 2015, <https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place/> (“So, building Google is roughly the equivalent of building the Windows operating system 40 times over. The [...] 2 billion lines that drive Google are *one thing*.”).

<sup>43</sup> CFIUS Questions for ByteDance/TikTok, August 26, 2021, pp. 13-14.

<sup>44</sup> See “Devpod: Improving Developer Productivity at Uber with Remote Development,” Uber, December 13, 2022, <https://www.uber.com/blog/devpod-improving-developer-productivity-at-uber/> (“Uber’s developer platform serves 5000 core software engineers to build, deploy, and manage high-quality software productively and at scale.”).

<sup>45</sup> As I described in paragraph 20, divestiture processes become more complex when the seller is less able (or willing) to support the divested asset post-divestiture, because if that is the case, the entirety of the operational effort must occur before closing. See also Eduardo Cuomo, “What Is Software Maintenance and Why Is It Important?,” Patagonian, March 22, 2023, <https://patagonian.com/blog/what-is-software-maintenance-and-why-is-it-important/> (“Cuomo, 2023”).

28. Fifth, even if Chinese export control laws did not forbid the divestment of certain elements of TikTok’s software, the preclusion of “any operational relationship” between Petitioners and the buyer means that the buyer must, upon divestiture, be prepared to engage in the “ongoing process” of “modifying, upgrading, and updating” the code underlying TikTok’s U.S. application without any post-divestiture support from Petitioners.<sup>46</sup> As I described above, Petitioners provided information to CFIUS indicating that TikTok has a large code base and development team,<sup>47</sup> and that TikTok’s software updates have a “high deployment frequency” with “approximately 1,000 backend service deployments to the TikTok application each day.”<sup>48</sup> TikTok’s large scale and deployment of frequent updates adds to the complexity of the divestiture because software maintenance—an undertaking “no less important than developing the software itself”—is an operational requirement for business continuity that, under the Act, could not be subject to a service agreement after January (or April) 19, 2025.<sup>49</sup>

29. Sixth, my opinion regarding the high level of integration and complexity of a “qualified divestiture” of TikTok’s U.S. application is unchanged by the technological and

---

<sup>46</sup> Cuomo, 2023. (“Software development is an ongoing process that requires constant optimization, even after the product is out in the market. [...] Software maintenance involves modifying, upgrading, and updating a software system to solve errors, improve the software itself, increase performance, or adapt the system to a change in conditions or the environment.”).

<sup>47</sup> See paragraph 27.

<sup>48</sup> CFIUS Questions for ByteDance/TikTok, August 26, 2021, p. 13. This level of deployments is on the order of Amazon, Google, Netflix, and Facebook. See Cate Lawrence, “Deployment Frequency – A Key Metric in DevOps,” Humanitec, February 4, 2021, <https://humanitec.com/blog/deployment-frequency-key-metric-in-devops> (“[An] elite group [of companies] routinely deploys on-demand and performs multiple deployments per day. [...] Amazon, Google, and Netflix deploy thousands of times per day (aggregated over the hundreds of services that comprise their production environments).”). See also Chuck Rossi, “Continuous Deployment of Mobile Software at Facebook (Showcase),” *2016 24th ACM SIGSOFT International Symposium*, November 2016 (“Given the size of Facebook’s engineering team, this resulted in 1,000’s of deployments into production each day.”).

<sup>49</sup> Cuomo, 2023. As I described in paragraph 20, divestiture processes become more complex when the seller is less able (or willing) to support the divested asset post-divestiture, because if that is the case, the entirety of the operational effort must occur before closing.

governance protections on which Petitioners have been working (dubbed “Project Texas”). I understand that Petitioners have been working on separating U.S. user data from non-U.S. user data, and that certain U.S. user data is stored in a protected enclave in the United States.<sup>50</sup> As part of Project Texas, ByteDance has established a special purpose subsidiary (TikTok U.S. Data Security Inc.) intended to (1) manage “all business functions that require access to U.S. user data identified by the U.S. government” and (2) safeguard “systems that deliver content on the app in the U.S. to ensure that it is free from foreign manipulation.”<sup>51</sup> However, I understand that neither TikTok U.S. Data Security Inc., nor any other technological and governance protections, have been intended to achieve a complete severing of all “operational relationships” between TikTok’s U.S. application and its global application.<sup>52</sup> I further understand that Project Texas does not contemplate the elimination of continued operational cooperation between TikTok’s U.S. application and ByteDance globally. For example, Project Texas contemplates TikTok’s U.S. application’s continued reliance on ByteDance engineers for certain fundamental parts of the code infrastructure that make the application work, including its recommendation engine.<sup>53</sup> Rather than duplicating these functions in the United States, Project Texas instead contemplates several layers of protection to validate and ensure the integrity of source code developed outside the United States.<sup>54</sup>

---

<sup>50</sup> “About Project Texas,” TikTok U.S. Data Security, <https://usds.tiktok.com/usds-about/> (“About Project Texas”).

<sup>51</sup> “About Project Texas”.

<sup>52</sup> “National Security Agreement CFIUS Case 20-100 Presentation to the Committee on Foreign Investment in the United States,” ByteDance/TikTok, September 8, 2023, (“NSA Presentation, 2023”), p. 16. *See also* “About Project Texas” *and* Matt Perault, “Has TikTok Implemented Project Texas?,” Lawfare, May 10, 2024, <https://www.lawfaremedia.org/article/has-tiktok-implemented-project-texas> (“Perault, 2024”).

<sup>53</sup> NSA Presentation, 2023, p. 16. *See also* “About Project Texas” *and* Perault, 2024.

<sup>54</sup> *See* “About Project Texas” *and* Perault, 2024.

30. For the above reasons, it is my opinion that any “qualified divestiture” of TikTok’s U.S. application would be highly complex.

**D. Market examples show that complex divestitures are time-consuming processes**

31. As I discussed above, the information that I have reviewed regarding a potential divestiture of TikTok’s U.S. application suggests that achieving a “qualified divestiture” would be highly complex. In this section I describe the time that highly complex divestitures take based on my: (1) experience with complex divestitures of highly integrated assets, and (2) evaluation of public information available on divestitures in the TMT sector. These examples indicate that the operational timeline alone of highly complex divestitures takes more than 360 days, *i.e.*, longer than the time afforded to Petitioners in the Act.

*1. My experience with Verizon’s divestitures illustrates the time-consuming and complex nature of divesting highly integrated assets*

32. The public often does not observe many of the divestiture steps that buyers and sellers conduct. For strategic reasons, companies often disclose information about a potential divestiture only after the parties have signed a binding agreement (and sometimes only after deal closing).<sup>55</sup> Similarly, the parties often do not disclose details regarding TSAs or other transition

---

<sup>55</sup> Zachary Turke and Edward Xia, “Why It’s Important to Manage Confidentiality in M&A Deals,” *Los Angeles & San Francisco Daily Journal*, August 31, 2020, [https://www.sheppardmullin.com/media/publication/1888\\_Sheppard%20DJ-8-31-2020\\_.pdf](https://www.sheppardmullin.com/media/publication/1888_Sheppard%20DJ-8-31-2020_.pdf), p. 1 (“Maintaining confidentiality of any information you disclose, including that a potential transaction might occur at all, is of the utmost importance.”).

agreements unless required to do so by law.<sup>56</sup> Therefore, the public typically only observes the divestiture timeline from the signing of a binding agreement until the close of the deal.

33. Companies in regulated industries, however, frequently face obligations to disclose details regarding their divestitures, providing transparency into otherwise concealed divestiture steps. Public records in regulated industries provide detail on the time and work that divestitures require and the associated complexity in the months and years after the divestiture.

34. Accordingly, my experience with three complex divestitures at Verizon, which operates in a regulated industry, allows me to describe comprehensively the time needed to separate and divest a highly integrated asset. These three Verizon divestitures, which I discuss below, illustrate the time-consuming and unpredictable nature of divesting highly integrated assets and the frequent provision of post-closing operational assistance by the seller to the buyer, irrespective of whether the buyer intends to integrate the divested assets into its existing business or to operate a new, stand-alone business.

35. These Verizon examples are relevant to evaluating any potential “qualified divestiture” of TikTok’s U.S. application because, pre-divestiture, the divested assets were highly integrated with the non-divested assets, as is the case between TikTok’s U.S. and global applications. Specifically:

- a. All three Verizon divestitures involved a geographic separation of a portion of Verizon’s business, instead of a more straightforward separation based on product

---

<sup>56</sup> As I discuss in **Section III.D**, public companies and companies in regulated industries frequently face obligations to disclose details regarding their divestitures, providing transparency into otherwise concealed divestiture steps.



market alone. Likewise, the divestiture required from Petitioners is a geographic separation of a portion of TikTok’s business.

- b. These assets had been highly integrated in Verizon’s overall business from a business-process perspective.<sup>57</sup> Likewise, TikTok’s U.S. application is an organic part of TikTok’s global application, meaning that the U.S. application is highly integrated in the global application.

36. The total timelines (inclusive of all corporate and operational steps) for these three Verizon divestitures took at least 751 days, 757 days, and 1,056 days, respectively—*i.e.*, each took between two and three times as long as the maximum timeline the Act affords Petitioners.<sup>58</sup> Importantly, the publicly observable operational timelines alone took at least 422, 727, and 642 days—all well over the time allotted to Petitioners by the Act. I summarize these Verizon divestitures below and provide more detail in **Appendix B**.

37. A 2005 divestiture of Verizon’s telephone access lines in Hawaii (“HawaiianTel”) spanned a total of 751 days between Verizon’s disclosure of deal discussions and the final operational cutover (*i.e.*, the date at which new stand-alone systems were up and running).<sup>59</sup> Furthermore, the operational timeline alone spanned at least 422 days—that is, longer than the

---

<sup>57</sup> See **Exhibit 1** and **Appendix B**.

<sup>58</sup> A total timeline of 751 days or 757 days is more than two times as long as the maximum timeline the Act affords to Petitioners (751 days / 360 days = 2.1; similarly, 757 days / 360 days = 2.1). A total timeline of 1,056 days is nearly three times as long as the maximum timeline the Act affords to Petitioners (1,056 days / 360 days = 2.9).

<sup>59</sup> The corporate timeline began on March 12, 2004 (when Verizon announced that it had been in divestment discussions), and it ended with the deal closing on May 2, 2005—representing a total of 417 days. See Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2003, p. 15; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2004, p. 16; Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7; “Verizon Hawaii, Inc. (GTHI),” Federal Communications Commission, <https://www.fcc.gov/verizon-hawaii-inc-gthi>.

time the Act affords Petitioners, without even considering the incremental corporate timeline.<sup>60</sup> Verizon and the buyer needed this 422-day period to handle the software challenges of splitting off highly integrated assets and establishing a stand-alone entity. Notably, after the transition began, the parties realized that they had underestimated the complexity of the software transition, and the TSA was extended.<sup>61</sup>

38. Similarly, Verizon's 2007 divestiture of its access lines in Maine, Vermont, and New Hampshire (*i.e.*, its Northeast Business), took 757 days between signing of the agreement and the final operational cutover.<sup>62</sup> The operational timeline alone took at least 727 days.<sup>63</sup>

---

<sup>60</sup> The operational timeline began on February 4, 2005, with the buyer's hiring of BearingPoint to create the necessary back-office systems for a new, stand-alone HawaiianTel and ended on April 1, 2006, when the final cutover to these systems occurred. *See* Decision and Order No. 21696, *In the Matter of the Application of Paradise Mergersub, Inc., GTE Corporation, Verizon Hawaii Inc., Bell Atlantic Communications, Inc., and Verizon Select Services Inc. for Approval of a Merger Transaction and Related Matters.*, No. 04-0140, <https://files.hawaii.gov/dcca/dca/dno/dno2005/21696.pdf>, p. 20; Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, pp. 50-51.

<sup>61</sup> The amendment to the initial agreement, dated December 15, 2005, extended the transition period for an additional 60 days to April 1, 2006. *See* Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7.

<sup>62</sup> The corporate timeline for this divestiture began on January 15, 2007, with the announcement of a deal between Verizon and FairPoint Communications, an established telecommunications provider, and ended on March 31, 2008, with the closing of the deal. *See* Agreement and Plan of Merger by and Among Verizon Communications Inc., Northern New England Spinco Inc., and FairPoint Communications, Inc., January 15, 2007; Joint Application for Approval of the Transfer of Certain Assets by Verizon New England Inc., Bell Atlantic Communications, Inc., NYNEX Long Distance Company, and Verizon Select Services Inc. and Associated Transactions; FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 2.

<sup>63</sup> The operational timeline largely overlapped with the corporate timeline and began on February 14, 2007, 30 days after the agreement was signed, when the planning for the transition started pursuant to the TSAs and Master Services Agreements (MSAs). (*See* Transition Services Agreement by and Among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-011/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>, p. 13 (“Within 30 calendar days following the date hereof [January 15, 2007, also when the Agreement and Plan of Merger was signed], the Cutover Planning Committee shall hold its initial meeting to commence planning and preparation for the Buyers to cease using all Transition Services and thereafter.”).) On February 9, 2009, FairPoint completed the cutover process and began operating its new systems independently from the Verizon systems. (*See* FairPoint Communications, Inc., Form 10-K for the Fiscal Year Ended December 31, 2008, pp. 2-3.)

Additionally, in September 2008, 595 days into the operational implementation, the parties realized that they had underestimated the complexity of the software transition, and despite a significant amount of pre-cutover system testing, the TSA services were extended.<sup>64</sup>

39. Lastly, Verizon’s 2009 divestiture of operations in 14 states (“14-State Divestiture”) to Frontier Communications Corporation (“Frontier”) spanned 1,056 days between signing of the agreement and the final operational cutover.<sup>65</sup> At least 642 days elapsed from deal closing to the final operational cutover, during which time underlying operations support was provided through a replica version of Verizon’s software until the operation support was migrated to Frontier’s own systems.<sup>66</sup>

40. These three Verizon divestitures illustrate the time-consuming and unpredictable nature of divesting highly integrated assets. In all cases, the operational timelines alone—at least 422, 727, and 642 days—were well over the time allotted to Petitioners by the Act, even if the

---

<sup>64</sup> FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 54 (“We expect to continue to require transition services agreement services from Verizon through January 2009, which is beyond the six month period following the closing of the merger, during which we anticipated requiring such services.”); *2009 Annual Report*, State of Maine Public Utilities Commission, February 1, 2010, <https://www.maine.gov/mpuc/sites/maine.gov/mpuc/files/inline-files/AR09-FINAL.pdf>, p. 11.

<sup>65</sup> The corporate timeline for the Frontier divestiture began no later than May 13, 2009, when the parties signed an agreement and ended with the closing of the deal on July 1, 2010. (*See* Memorandum Opinion and Order, *In the Matter of Applications Filed by Frontier Communications Corporation and Verizon Communications Inc. for Assignment or Transfer of Control*, WC Docket No. 09-95, May 21, 2010, p. 4; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2010, Note 3; “Verizon Completes Spinoff of Local Exchange Businesses and Related Landline Activities in 14 States,” Verizon News Archives, July 1, 2010, <https://www.verizon.com/about/news/press-releases/verizon-completes-spinoff-local-exchange-businesses-and-related-landline-activities-14-states>.) Frontier completed the integration of operations from Verizon in April 2012. (*See* Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>.)

<sup>66</sup> Frontier completed the integration of operations from Verizon on April 2, 2012. *See* Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>; Memorandum Opinion and Order, *In the Matter of Applications Filed for the Transfer of Certain Spectrum Licenses and Section 214 Authorizations in the States of Maine, New Hampshire, and Vermont from Verizon Communications Inc. and Its Subsidiaries to FairPoint Communications, Inc.*, WC Docket No. 07-22, January 9, 2008, p. 12.

President were to grant an extension to April 2025. In both the 2007 and 2009 divestitures, the operational time alone that Verizon needed to execute the divestiture nearly doubled the maximum amount of time afforded to Petitioners by the Act.<sup>67</sup>

2. *Other high-value divestitures in the TMT sector illustrate the length and complexity of divesting highly integrated assets*

41. My evaluation of additional divestitures in the TMT sector further corroborates my conclusion that complex divestitures with highly integrated assets take longer than the time the Act affords to Petitioners.<sup>68</sup> Additionally, as I show below, even divestitures of less integrated assets in this sector often take longer than the time afforded to Petitioners in the Act.

42. I used a two-step process to identify comparable historical divestitures. First, I used S&P Capital IQ Pro—the research division of one of the largest providers of financial information<sup>69</sup>—to identify historical divestiture transactions that satisfied the following criteria:<sup>70</sup>

- a. The divested assets operated in the “interactive media and services,” “application software,” “systems software,” or “integrated telecommunication services” industries;<sup>71</sup>

---

<sup>67</sup> An operational timeline of 727 days or 642 days is nearly two times as long as the maximum timeline the Act affords to Petitioners (727 days / 360 days = 2.0; similarly, 642 days / 360 days = 1.8).

<sup>68</sup> As I describe below, S&P Capital IQ Pro classifies TikTok Inc. as part of the “Technology, Media & Telecommunications” sector.

<sup>69</sup> James Chen, “S&P Capital IQ Definition, Products and Services,” Investopedia, April 30, 2024, <https://www.investopedia.com/terms/c/capital-iq.asp>.

<sup>70</sup> To identify divestiture transactions in S&P Capital IQ Pro, I used the filter “Transaction Type” to select transactions that were either “M&A - Asset” or “M&A - Spinoff or Splitoff.”

<sup>71</sup> S&P Capital IQ Pro classifies TikTok Inc. as part of the “interactive media and services” industry within the “Technology, Media & Telecommunications” sector. Therefore, I limited my research to transactions that involved divested assets operating in the “interactive media and services” industry as well as other industries within the “Technology, Media & Telecommunications” sector that are related to TikTok. For example, I included the industry that S&P Capital IQ Pro uses to classify ByteDance Ltd (“application software”) and

- b. The transaction (1) took place in the United States,<sup>72</sup> (2) was announced and completed in the last ten years (between 2014 and 2024),<sup>73</sup> and (3) had a total transaction value greater than \$1 billion;<sup>74</sup> and
- c. At least one of either the buyer or the seller had publicly available Securities and Exchange Commission (“SEC”) filings at the time of the divestiture, and the transaction was subject to regulatory or antitrust approval.<sup>75</sup>

43. Including in the selection criteria that at least one of the parties had publicly available SEC filings and that the transaction was subject to regulatory or antitrust approval allowed me, in most cases, to retrieve relevant information (such as information on TSAs) to determine an operational timeline that might otherwise be concealed from the public. I found 26 divestitures that satisfied the above criteria and I refer to these 26 divestitures as my “market sample.”<sup>76</sup>

---

industries that are closely related to application software (“systems software” or “integrated telecommunication services”).

<sup>72</sup> Specifically, in S&P Capital IQ Pro, I used the filter “Transaction Geography” to select “United States.”

<sup>73</sup> Specifically, in S&P Capital IQ Pro, I used the filter “Announced Date” to select these dates and the filter “Transaction Status” to require that the transaction was “Completed.”

<sup>74</sup> Specifically, in S&P Capital IQ Pro, I set the data field “Total Transaction Value (\$M)” to be greater than \$1 billion. I used the \$1 billion cutoff because publicly available information indicates that the TikTok transaction would be over \$1 billion. *See, e.g.*, Dylan Butts, “Kevin O’Leary Wants to Buy TikTok at Up to 90% Discount. Here’s Why,” CNBC, March 22, 2024, <https://www.cnbc.com/2024/03/22/kevin-oleary-on-why-he-wants-to-buy-tiktok-.html>; Brian Fung, “Who Could Buy TikTok?,” CNN Business, April 25, 2024, <https://www.cnn.com/2024/04/25/tech/who-could-buy-tiktok/index.html> (describing a value of \$20 billion to \$30 billion); Natalie Andrews et al., “TikTok Crackdown Shifts Into Overdrive, with Sale or Shutdown on Table,” The Wall Street Journal, March 10, 2024, <https://www.wsj.com/tech/why-the-new-effort-to-ban-tiktok-caught-fire-with-lawmakers-7cd3f980> (describing a price tag “in the hundreds of billions of dollars”). With that said, my results hold even if I lower the cutoff to \$750 million.

<sup>75</sup> Specifically, in S&P Capital IQ Pro, I used the filter “deal condition” to select transactions that are classified as reporting a divestiture subject to “Regulatory or Antitrust Approval” (*e.g.*, subject to competition authority approval).

<sup>76</sup> My analysis of these 26 divestitures is presented in **Exhibit 1**.

44. Second, to limit my market sample to transactions that involved divestitures of highly integrated assets, I excluded transactions for which either: (1) the divested asset was defined solely based on product market, or (2) the seller acquired the divested asset within ten years of the evaluated divestiture.<sup>77</sup> The four divestitures that remained were:

- a. Lumen Technologies Inc.'s ("Lumen") 2022 sale of its local exchange business, valued at \$7.5 billion,<sup>78</sup> to Apollo Global Management ("Apollo");<sup>79</sup>
- b. Frontier's 2020 sale of some of its operations and assets, valued at \$1.35 billion, to a group of financial investors;<sup>80</sup>

<sup>77</sup> I described the rationale behind these criteria in **Section III.B**.

<sup>78</sup> Here and in the remainder of my declaration, I report transaction values as shown by S&P Capital IQ Pro.

<sup>79</sup> In Lumen's case, geographic considerations were necessary to define the divested asset because Lumen divested its operations in some states while retaining the same operations (*i.e.*, same products supported by common systems) in some other states. The public record that I have reviewed indicates that Lumen did not acquire the divested asset within ten years before the evaluated divestiture. "Lumen to Sell Local Incumbent Carrier Operations in 20 States to Apollo Funds for \$7.5 Billion," PR Newswire, August 3, 2021, <https://www.prnewswire.com/news-releases/lumen-to-sell-local-incumbent-carrier-operations-in-20-states-to-apollo-funds-for-7-5-billion-301347625.html>.

<sup>80</sup> In Frontier's case, geographic considerations were necessary to define the divested asset because Frontier divested its operations in some states while retaining the same operations (*i.e.*, same products supported by common systems) in some other states. (Matt Pilon, "Frontier Unloads Northwest Telecom Assets for \$1.35B," HBJ, May 29, 2019, <https://www.hartfordbusiness.com/article/frontier-unloads-northwest-telecom-assets-for-135b>.) The public record that I have reviewed indicates that Frontier did not acquire the divested asset within ten years before the evaluated divestiture. Although Frontier acquired Verizon's wireline operations in Washington, Oregon, and Idaho in the 14-State Divestiture in 2010, the asset divested in 2019 was different than those acquired in 2010. First, the divested asset included Frontier's wireline operations in Montana, which it did not acquire from Verizon. (*See* "California, Nevada and South Carolina Approve Frontier Acquisition of Verizon Local Wireline Operations," Verizon News Archives, October 29, 2009, <https://www.verizon.com/about/news/press-releases/california-nevada-and-south-carolina-approve-frontier-acquisition-verizon-local-wireline-operations>.) Second, the divested asset included the lines that Frontier operated in Oregon and Idaho prior to the 2010 14-State Divestiture, which were subsequently integrated with the operations purchased from Verizon. (*See* "Frontier Communications Announces Sale of Operations in Washington, Oregon, Idaho, and Montana," Frontier Communications, May 29, 2019, <https://investor.frontier.com/news/news-details/2019/Frontier-Communications-Announces-Sale-of-Operations-in-Washington-Oregon-Idaho-and-Montana-05-29-2019/default.aspx>; Citizens Communications Company, Form 10-K for the Fiscal Year Ended December 31, 2006, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/c1dd8f8d-65be-4a83-b357-0075cbe1fe54.pdf>, Exhibit 21.)

- c. CDK Global Inc.’s (“CDK”) 2021 sale of its international business, valued at \$1.45 billion, to Francisco Partners Management (“Francisco”);<sup>81</sup> and
- d. Verizon’s 2016 sale of certain additional wireline operations, valued at \$10.54 billion, to Frontier.<sup>82,83</sup>

45. The operational timelines alone of each of these four divestitures (701 days, 459 days, 432 days, and 398 days, respectively) took longer than the maximum of 360 days that the Act affords to Petitioners.<sup>84</sup> Moreover, consistent with the divested assets’ high level of pre-divestiture integration, each of these divestitures included a TSA or other forms of technological support services following deal close. As I described above, TSAs and similar technological

---

<sup>81</sup> In CDK’s case, geographic considerations were necessary to define the divested asset because CDK divested its business in EMEA and Asia while retaining operations for the same products in other geographies. (*See* “Francisco Partners to Acquire International Business of CDK Global for \$1.45 Billion,” Francisco Partners, November 30, 2020, <https://www.franciscopartners.com/media/francisco-partners-to-acquire-international-business-of-cdk-global-for-145-billion>.) The public record that I have reviewed indicates that CDK did not acquire the divested asset within ten years before the evaluated divestiture. Although ADP spun off CDK in 2014, this spin-off is irrelevant when evaluating CDK’s 2021 divestiture of its international business. This is because, in 2021, CDK sold only one division of CDK (*i.e.*, its international business), rather than the entire entity that was spun off in 2014. Therefore, in 2021, CDK had to disentangle its international business from the rest of the entity. For this reason, the divested asset (*i.e.*, the international business) was not an asset that was acquired within 10 years of the announcement date. (*See* John Kirwan, “International Business of CDK Global Becomes Keyloop,” MotorTrader.com, March 1, 2021, <https://www.motortrader.com/motor-trader-news/automotive-news/307888-01-03-2021>.)

<sup>82</sup> In Verizon’s case, geographic considerations were necessary to define the divested asset because Verizon divested its operations in some states while retaining the same operations (*i.e.*, same products supported by common systems) in some other states. The public record that I have reviewed indicates that Verizon did not acquire the divested asset within ten years before the evaluated divestiture. *See* “Frontier Communications Completes Acquisition of Verizon Wireline Operations in California, Texas and Florida,” April 1, 2016, <https://investor.frontier.com/news/news-details/2016/Frontier-Communications-Completes-Acquisition-of-Verizon-Wireline-Operations-in-California-Texas-and-Florida-04-01-2016/default.aspx>.

<sup>83</sup> Because this Verizon divestiture took place after I left Verizon, I do not have personal experience with this transaction. For this reason, I describe this divestiture in **Section III.D.2** instead of **Section III.D.1** (where I discussed other Verizon divestitures with which I am personally familiar).

<sup>84</sup> The corporate timeline alone of these divestitures (427, 339, 92, and 422 days, respectively) were similarly lengthy. However, as I described in **Section III.A**, I do not consider corporate timelines in my analysis because I have taken the conservative assumption in my declaration that TikTok would be able to achieve a corporate timeline of zero days.

support service agreements are not ideal for the seller or the buyer; therefore, the parties had an incentive to keep the observed operational timelines as short as possible.

- a. Lumen provided transition services to Apollo for “an average of 17 months [with the] right to extend the term of certain services for up to six months,” or up to 701 days.<sup>85</sup>
- b. Frontier agreed to provide “various network and support services”<sup>86</sup> as well as “limited training and subject matter support services”<sup>87</sup> on July 31, 2019, and provided these services until October 31, 2020, or approximately 459 days.<sup>88</sup>
- c. CDK entered a TSA with Fransico in November 2020 to assist in the integration of the international business.<sup>89</sup> CDK provided these services to Fransico until February 2022, for approximately 432 days.<sup>90</sup>

---

<sup>85</sup> “Under the TSA, Lumen actually began providing transition services upon the October 3, 2022, completion date of the Divestiture. [...] The term of services to be provided under the TSA is an average of 17 months, subject to Apollo’s right to extend the term of certain services for up to six months and to terminate early the term of any service.” See Lumen Technologies, Inc., Form 8-K, dated October 3, 2022, <http://pdf.secdatabase.com/1788/0001193125-22-256669.pdf>.

<sup>86</sup> Frontier Communications, Form 10-K for the Fiscal Year Ended December 31, 2019, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/b7334365-f330-4e9d-8f5b-850623fd18d8.pdf>, p. 2.

<sup>87</sup> Frontier Communications, Form 10-K for the Fiscal Year Ended December 31, 2020, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/6b950dad-b24b-4079-ae7e-b089a4f71e59.pdf>, F-29.

<sup>88</sup> Frontier committed to planning the transition of operations at least as early as July 31, 2019. Testimony of Steve Weed, No. UT-190574, July 31, 2019, p. 37 (“Frontier has agreed to replicate its current IT systems”). Frontier stated that it stopped providing the services regulated by the TSA as of October 31, 2020.

<sup>89</sup> The TSA is attached to the Share Sale and Purchase Agreement dated November 27, 2020. Share Sale and Purchase Agreement by and Among CDK Global Holdings Ltd., the Other Restricted Entities Party Hereto, and Concorde Bidco Ltd., dated November 27, 2020, [https://www.sec.gov/Archives/edgar/data/1609702/000160970221000005/cdk\\_q2fy21concorde-sharesa.htm](https://www.sec.gov/Archives/edgar/data/1609702/000160970221000005/cdk_q2fy21concorde-sharesa.htm).

<sup>90</sup> CDK Global, Inc., Form 10-Q for the Quarterly Period Ended March 31, 2022, p. 10. As the precise end date is unknown, I conservatively assumed that CDK’s transition services ended on February 1, 2022.



- d. Verizon entered a support agreement with Frontier in February 2015,<sup>91</sup> and the transaction closed on April 1, 2016,<sup>92</sup> *i.e.*, 398 days later.<sup>93</sup>

46. These examples provide further evidence that divestitures of highly integrated assets: (1) consistently take more than 360 days; and (2) often necessitate post-closing services provided by the seller to the buyer to ensure business continuity. I note that—while these divestitures shared two indicia of complexity with the divestiture required of Petitioners (*i.e.*, a geographically defined divestiture of organically developed assets or assets held over ten years)—as I described in **Section III.C**, there are additional indicia of complexity associated with divesting TikTok’s U.S. application.

47. Additionally, **Exhibit 1** shows that, even when a divestiture involves assets that appear to be less integrated than TikTok’s U.S. application, the operational timelines for divestitures in the software industry (and in other industries within the TMT sector) nevertheless often take over 360 days.

---

<sup>91</sup> The support agreement provided that the parties would develop a “joint Cutover Plan to set forth the processes, procedures, and steps through which the parties would prepare for and effect the cutover [*i.e.*, the switch from Verizon to Frontier following deal closing].” The parties “spent months” developing a 300-page plan (which created approximately 140 functional working teams, including teams from Engineering and IT). Response of Frontier California Inc. (U 1002 C) to Assigned Commissioner’s Ruling Inviting Party and Public Comments Regarding Issues Raised at Public Participation Hearings and Workshops in the Intrastate Rural Call Completion Issues Proceeding (I.14-05-012), September 20, 2016, <https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M168/K257/168257703.PDF>, Attachment A.

<sup>92</sup> Frontier CPED Settlement Agreement, December 19, 2019, <https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M472/K024/472024199.pdf>, p. 2 (“[T]he transaction closed on April 1, 2016, and Frontier implemented a ‘cutover plan’ to transition the Verizon customers to Frontier’s service platform”).

<sup>93</sup> I conservatively assumed the start of the operational timeline March 1, 2015, *i.e.*, the first day after the cutover plan support agreement was entered. I considered the end of the operational timeline, April 1, 2016, the transaction close date. The resulting 398 days are consistent with a 2019 settlement agreement stating that “Frontier had been planning the transition for more than a year[.]” Frontier CPED Settlement Agreement, December 19, 2019, <https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M472/K024/472024199.pdf>, p. 2.

48. The 22 transactions remaining in my market sample all have indicia of less integration—and hence less complexity—than the four divestitures described above (as well as the three divestitures from Verizon that I personally experienced). In other words, each of the 22 remaining transactions involved either: (1) a divested asset defined solely by product market, or (2) the divestiture of an asset acquired within ten years of divestiture, or (3) both of these conditions.<sup>94</sup> Nevertheless, for these divestitures that have the indicia of less complexity than TikTok, the range of operational timelines often extended beyond 360 days.

49. For example, in the following eight divestitures, the divested asset was defined based solely on product market (*i.e.*, they have one of the indicia of a less complex divestiture than the divestiture required of Petitioners), and yet their expected or observable operational timelines were longer than 360 days:<sup>95</sup>

---

<sup>94</sup> As shown in **Exhibit 1** and below, my market sample included no divestitures where the seller acquired the divested asset within ten years *and* the divested asset was defined solely by product market.

<sup>95</sup> For some divestitures in my market sample, I found information indicating the *de facto* operational timeline (*e.g.*, the beginning of planning activities as the observable start date, and the end of assistance provided by the seller as the observable end date of the operational timeline). For other divestitures in my sample, I found information only regarding the *de jure* operational timeline (*e.g.*, TSAs or similar documents including the time the parties expected it would take for the seller to provide transition services, *i.e.*, the *expected* operational timeline), without the *de facto* end date of the operational timeline. For this reason, I describe the operational timelines here as “expected or observable.” Given that—based on my experience and the literature (described above)—operational timelines are frequently underestimated, relying on the expected time presented in the TSA is likely a conservative estimate of the *de facto* operational timeline. For the same reason, where the available information provided a range as the expected operational timeline, I rely on the upper end of the range (while presenting the full range in **Exhibit 1**). *See, e.g.*, Yetton 2023, at p. 962 (“IT carve-out projects are notoriously problematic. IT carve-out projects frequently overrun timelines and budgets [...]. In part, this is because IT carve-out projects are frequently under-planned and underestimated”).

- a. Thomson Reuters Corporation’s 2016 divestiture of its intellectual property and science business, valued at \$3.55 billion,<sup>96</sup> to Onex Corporation (operational timeline of 1,087 days).<sup>97</sup>
- b. IAC Holdings, Inc.’s 2020 spin-off of Match Group, Inc., valued at \$8.09 billion<sup>98</sup> (operational timeline of 732 days);<sup>99</sup>

---

<sup>96</sup> See “Thomson Reuters Announces Definitive Agreement to Sell Its Intellectual Property & Science Business to Onex and Baring Asia for \$3.55 Billion,” PR Newswire, July 11, 2016, <https://www.prnewswire.com/news-releases/thomson-reuters-announces-definitive-agreement-to-sell-its-intellectual-property--science-business-to-onex-and-baring-asia-for-355-billion-300296352.html>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>97</sup> I considered the start of the operational timeline the date of the TSA, July 10, 2016. I conservatively assumed the end of the operational timeline to be July 1, 2019, because the buyer recorded “payments to Thomson Reuters under the [TSA]” during the three months ended on September 30, 2019. See “Clarivate Analytics Reports Third Quarter 2019 Results,” Clarivate Analytics, November 6, 2019, <https://clarivate.com/news/clarivate-analytics-reports-third-quarter-2019-results/>.

<sup>98</sup> See “IAC and Match Group Complete Full Separation,” IAC, July 1, 2020, <https://www.iac.com/press-releases/iac-and-match-group-complete-full-separation>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture. Match.com was acquired by TMCS (Ticketmaster Online-CitySearch Inc.) in June 1999 (*i.e.*, more than ten years before this divestiture’s announcement date). In 2003 (still more than ten years before this divestiture’s announcement date), IAC acquired TMCS, and following Match.com’s IPO on November 24, 2014, IAC retained a significant stake in the company. See “25 Year Innovator,” IAC, <https://www.iac.com/history>; “IAC and Match Group Announce Closing of Initial Public Offering,” IAC, November 24, 2015, <https://www.iac.com/press-releases/iac-and-match-group-announce-closing-of-initial-public-offering>.

<sup>99</sup> I considered the start of the operational timeline the date of the TSA, June 30, 2020. (See IAC/InterActiveCorp and IAC Holdings, Inc., Transition Services Agreement by and Between IAC/InterActiveCorp and IAC Holdings, Inc., dated June 30, 2020, [https://www.sec.gov/Archives/edgar/data/1800227/000110465920080610/tm2022502d7\\_ex10-1.htm](https://www.sec.gov/Archives/edgar/data/1800227/000110465920080610/tm2022502d7_ex10-1.htm).) I conservatively assumed the end of the operational timeline to be July 1, 2022, because the seller recorded revenues “from IAC for services provided to IAC under the transition services agreement” during the three-month period ended September 30, 2022. Match Group, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2022, dated November 4, 2022, <https://www.sec.gov/Archives/edgar/data/891103/000089110322000095/mtch-20220930.htm>, p. 27.

- c. IAC Inc.’s 2021 spin-off of Vimeo, Inc., valued at \$7.68 billion<sup>100</sup> (operational timeline of at least 588 days);<sup>101</sup>
- d. SolarWinds Corporation’s 2021 spin-off of its Managed Service Provider (MSP) business into N-able, Inc., valued at \$2.05 billion<sup>102</sup> (expected operational timeline of 534 days);<sup>103</sup>

<sup>100</sup> See “IAC Completes Spin-Off Of Vimeo,” IAC, May 25, 2021, <https://www.iac.com/press-releases/iac-completes-spin-off-of-vimeo>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>101</sup> I considered the start of the operational timeline the date of the TSA, May 24, 2021. I made the conservative assumption that the end of the operational timeline is January 1, 2023, because, as of at least January 1, 2023, IAC continued to receive fees “for services rendered pursuant to the transition services agreement.” See IAC/InterActiveCorp and Vimeo, Inc., Transition Services Agreement by and Between IAC/InterActiveCorp and Vimeo, Inc., dated May 24, 2021, [https://www.sec.gov/Archives/edgar/data/1837686/000110465921073207/tm2117737d1\\_ex10-3.htm](https://www.sec.gov/Archives/edgar/data/1837686/000110465921073207/tm2117737d1_ex10-3.htm); IAC/InterActiveCorp and Vimeo, Inc., Extension Request #2 Pursuant to Transition Services Agreement by and Between IAC/InterActiveCorp and Vimeo, Inc., dated June 30, 2022, <https://www.sec.gov/Archives/edgar/data/1837686/000183768622000022/ex101-2022630.htm>; IAC Inc., Form 10-Q for the Quarterly Period Ended March 31, 2023, <https://www.sec.gov/Archives/edgar/data/1800227/000180022723000016/iaci-20230331.htm>.

<sup>102</sup> See “SolarWinds Completes Spin-Off of its MSP Business; N-able, Inc. Begins Trading as Independent, Publicly Traded Company,” SolarWinds, July 20, 2021, <https://investors.solarwinds.com/news/news-details/2021/SolarWinds-Completes-Spin-Off-of-its-MSP-Business-N-able-Inc.-Begins-Trading-as-Independent-Publicly-Traded-Company/default.aspx>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture. I note that SolarWinds’ 2013 acquisition of a *different* company that was also called “N-able” is irrelevant for this evaluation. Following this 2013 acquisition, SolarWinds integrated the assets of N-able with the assets of another company that SolarWinds acquired in 2016 (LOGICnow) to create “SolarWindsMSP.” Then, in 2021, SolarWinds spun off “SolarWindsMSP” as a new entity, which SolarWinds named “N-able.” See Stefanie Hammond, “Happy anniversary to me!,” N-able, November 24, 2021, <https://www.n-able.com/fr/blog/happy-anniversary-to-me>.

<sup>103</sup> The TSA was dated as of July 16, 2021, and the transition services were expected to end on December 31, 2022. See Transition Services Agreement by and Between SolarWinds Corporation and N-Able, Inc., dated July 16, 2021, <https://www.sec.gov/Archives/edgar/data/1739942/000162828021014064/exhibit101-swinxable8xk.htm>. See also SolarWinds Corporation, Form 10-K for the Fiscal Year Ended December 31, 2021, <https://www.sec.gov/Archives/edgar/data/1739942/000173994222000020/swi-20211231.htm>, p. F-36 (“The transition services agreement will terminate on the expiration of the term of the last service provided under it, which SolarWinds anticipates to be on or around December 31, 2022.”).

- e. Micro Focus International plc’s 2017 acquisition of Hewlett Packard’s software business, valued at \$9.00 billion<sup>104</sup> (expected operational timeline of up to 456 days);<sup>105</sup>
- f. Automatic Data Processing, Inc.’s 2014 spin-off of its automotive dealer services product business, valued at \$4.94 billion<sup>106</sup> (operational timeline of at least 367 days);<sup>107</sup>

<sup>104</sup> “UK Tech Giant Micro Focus Plunges in Value as Shares Crash,” BBC, March 19, 2018, <https://www.bbc.com/news/business-43457024> (Micro Focus International plc “purchase[d] [...] Hewlett Packard Enterprise’s software business for £6.8bn.”). I used the U.S. dollar value of \$9.00 billion as reported by S&P Capital IQ Pro. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>105</sup> See Transition Services Agreement by and Between Hewlett Packard Enterprise Company and Seattle SpinCo, Inc., dated September 1, 2017, [https://www.sec.gov/Archives/edgar/data/1645590/000156761917001826/s001851x1\\_ex2-3.htm](https://www.sec.gov/Archives/edgar/data/1645590/000156761917001826/s001851x1_ex2-3.htm); Seattle SpinCo, Inc. and Micro Focus International plc, Form 424B3, dated August 15, 2017, [https://www.sec.gov/Archives/edgar/data/1359711/000156761917001747/s001838x1\\_424b3.html](https://www.sec.gov/Archives/edgar/data/1359711/000156761917001747/s001838x1_424b3.html)149, p. 219 (“The initial term of the Transition Services Agreement will be nine months, and each party in certain circumstances may extend the term of services it will receive for up to two three-month periods (for a total term of up to 15 months)”).

<sup>106</sup> See “ADP Completes Spin-Off of Automotive Dealer Services Business,” Paul Weiss, September 30, 2014, <https://www.paulweiss.com/practices/transactional/corporate/news/adp-completes-spin-off-of-automotive-dealer-services-business?id=18827> (“Automatic Data Processing, Inc. (ADP) completed the distribution to its stockholders of all of the issued and outstanding common stock of CDK Global, Inc. in a tax-free spin-off. The distribution completes the spin-off by ADP of its automotive dealer services business”). The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>107</sup> I considered the start of the operational timeline the date of the TSA, September 29, 2014. I considered the end of the operational timeline September 30, 2015, the last date of the transitional period “pursuant to the transition services agreement” with ADP. See CDK Global, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2014, [https://www.sec.gov/Archives/edgar/data/1609702/000160970214000006/cdk\\_q1fy1510-q.htm](https://www.sec.gov/Archives/edgar/data/1609702/000160970214000006/cdk_q1fy1510-q.htm), p. 34; CDK Global, Inc., Form 10-Q for the Quarterly Period Ended December 31, 2015, [https://www.sec.gov/Archives/edgar/data/1609702/000160970216000037/cdk\\_q2fy1610-q.htm](https://www.sec.gov/Archives/edgar/data/1609702/000160970216000037/cdk_q2fy1610-q.htm), p. 7.

- g. Symantec Corporation’s 2017 divestiture of its website security business, valued at \$1.12 billion,<sup>108</sup> to DigiCert, Inc. (operational timeline of at least 365);<sup>109</sup> and
- h. IBM Corporation’s 2019 divestiture of its software portfolio of international business, valued at \$1.78 billion,<sup>110</sup> to HCL Technologies Ltd. (expected operational timeline up to over 365 days).<sup>111</sup>

50. Similarly, in the following five divestitures, the divested asset was defined based solely on product market *and* the seller acquired the divested asset within ten years before the divestiture (*i.e.*, they have both indicia of a less complex divestiture than the one required of

<sup>108</sup> See John Merrill, “DigiCert to Acquire Symantec’s Website Security Business,” DigiCert, August 2, 2017, <https://www.digicert.com/blog/digicert-to-acquire-symantec-website-security-business>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>109</sup> See Purchase Agreement by and Among Symantec Corporation, DigiCert Parent, Inc., and DigiCert, Inc., dated August 2, 2017, <https://www.sec.gov/Archives/edgar/data/849399/000084939917000016/a092917exhibit21.htm>, pp. 111-112 (“Unless otherwise agreed by Arion (refers to DigiCert) and Sphinx (refers to Symantec) or set forth in the Preliminary Transition Service Schedules, no Transition Period will last for more than 12 months following the Closing Date (excluding any extensions made to the Transition Period in accordance with the terms of the Transition Services Agreement”). See also Symantec Corporation, Form 10-Q for the Quarterly Period Ended December 29, 2017, <https://www.sec.gov/Archives/edgar/data/849399/000084939918000004/symc122917-10q.htm>, p. 14 (“The services under the TSA commenced with the close of the transaction and expire at various dates through fiscal 2019, with extension options”).

<sup>110</sup> See “HCL Technologies to Buy IBM Software Products in \$1.8 Billion Deal,” Nikkei Asia, December 7, 2018, <https://asia.nikkei.com/Business/Companies/HCL-Technologies-to-buy-IBM-software-products-in-1.8-billion-deal>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>111</sup> For the lower bound of the operational timeline, I conservatively assumed that the start date is January 31, 2019, because HCL Tech announced in January 2019 that “HCL is working on a smooth transition plan.” As the end date, I conservatively used the date of the deal close, June 30, 2019. For the upper bound, I conservatively used 365 days because IBM stated that “HCL can renew certain [transition] services up to an additional year.” See “HCL Announces Acquisition of Select IBM Products Frequently Asked Questions,” Products & Platforms, [https://www.hcltech.com/sites/default/files/documents/inline-migration/general\\_faq\\_jan\\_2019.pdf](https://www.hcltech.com/sites/default/files/documents/inline-migration/general_faq_jan_2019.pdf), p. 3; IBM Corporation, Form 10-Q for the Quarter Ended September 30, 2019, <https://www.sec.gov/Archives/edgar/data/51143/000155837019009324/ibm-20190930x10q.htm>, p. 52.

Petitioners), and yet they too have expected or observable operational timelines longer than 360 days:

- a. Xperi Holding Corporation's 2022 spin-off of its product business from its intellectual property licensing business, valued at \$1.08 billion<sup>112</sup> (operational timeline of at least 844 days);<sup>113</sup>
- b. TEGNA Inc.'s 2017 spin-off of Cars.com Inc., valued at \$1.85 billion<sup>114</sup> (operational timeline of up to 24 months, *i.e.*, 730 days);<sup>115</sup>

---

<sup>112</sup> Xperi (formerly Tessera Holding Corporation) acquired the product business of DTS, Inc in December 2016, *i.e.*, six years before this divestiture. (See "Tessera Completes Acquisition of DTS," Business Wire, December 1, 2016, <https://www.businesswire.com/news/home/20161201005268/en/Tessera>; "Tessera Holding Corporation Announces Name Change to Xperi Corporation," Xperi, February 22, 2017, <https://investor.xperi.com/news/news-details/2017/Tessera-Holding-Corporation-Announces-Name-Change-to-Xperi-Corporation/default.aspx>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

<sup>113</sup> While I have found neither the precise start date nor the precise end date of the operational timeline from public documents, I was able to estimate the operational timeline by using conservative proxy dates for both. As the start date, I used July 1, 2020, which is the first day following the month in which Xperi publicly announced its intention to divest its assets (June 2020). Using this date as the start of the operational timeline is conservative because public announcements typically occur following internal operational planning. As the end date, I used October 22, 2022, the date of the first amendment to the TSA. This date is conservative as the implementation of the TSA is likely to continue after its amendment date. See Xperi Inc., Form 10-K for the Fiscal Year Ended December 31, 2023, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001788999/0768588f-717f-4908-a897-745524c9f289.pdf>, pp. 51-52; Xperi Inc., Form 10-K for the Fiscal Year Ended December 31, 2022, <https://www.sec.gov/ix?doc=/Archives/edgar/data/1788999/000095017023006053/xper-20221231.htm>, p. 105.

<sup>114</sup> See "Cars.com Completes Spin-off from Parent Company TEGNA," Cars.com, June 1, 2017, <https://www.cars.com/articles/carscom-completes-spin-off-from-parent-company-tegna-1420695567172/>. Gannett, the corporate predecessor of TEGNA, acquired Cars.com in 2014, *i.e.*, three years before this divestiture. (See Veronica Garabelli, "Gannett Acquires Cars.com for \$1.8 Billion," Virginia Business, October 1, 2014, <https://www.virginiabusiness.com/article/gannett-acquires-cars-com-for-1-8-billion/>; "Separation of Gannett into Two Public Companies Completed," TEGNA, June 29, 2015, <https://www.tegna.com/separation-of-gannett-into-two-public-companies-completed/>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

<sup>115</sup> TEGNA and Cars.com entered a TSA on May 31, 2017, pursuant to which TEGNA agreed to "provide certain services to Cars.com on an interim and transitional basis, not to exceed 24 months." See Transition Services Agreement by and Between TEGNA Inc. and Cars.com Inc., dated May 31, 2017, <https://www.sec.gov/Archives/edgar/data/39899/000119312517196074/d514170dex101.htm>; TEGNA Inc., Form 10-Q for the Quarterly Period Ended September 30, 2017, <https://www.sec.gov/Archives/edgar/data/39899/000003989917000041/tgna-20170930x10q.htm>, p.20.

- c. FireEye, Inc.’s 2021 divestiture of its products business, valued at \$1.2 billion,<sup>116</sup> to Symphony Technology Group (expected operational timeline of up to 548 days);<sup>117</sup>
- d. Dell Technologies Inc.’s 2021 spin-off of VMware LLC, valued at \$51.14 billion<sup>118</sup> (expected operational timeline of up to 365 days);<sup>119</sup>

<sup>116</sup> See “FireEye Announces Sale of FireEye Products Business to Symphony Technology Group for \$1.2 Billion,” Mandiant, June 2, 2021, <https://www.mandiant.com/company/press-releases/fireeye-announces-sale-fireeye-products-business-symphony-technology-group>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. See Zacks Equity Research, “FireEye Rebrands as Mandiant (FEYE) After Product Biz Sell-Off,” Nasdaq, October 5, 2021, <https://www.nasdaq.com/articles/fireeye-rebrands-as-mandiant-feye-after-product-biz-sell-off-2021-10-05> (“Through this transaction, [FireEye] undoes its 2014 acquisition, which brought Mandiant solutions and FireEye products together”).

<sup>117</sup> On June 2, 2021, FireEye said it would enter a TSA at closing. See FireEye, Symphony Technology Group, FireEye Announces Sale of FireEye Products Business to Symphony Technology Group for \$1.2 Billion, [https://www.sec.gov/Archives/edgar/data/1370880/000110465921075725/tm2118082d1\\_ex99-1.htm](https://www.sec.gov/Archives/edgar/data/1370880/000110465921075725/tm2118082d1_ex99-1.htm) (“[FireEye] at closing will enter into agreements [which] include [...] a transition services agreement”); FireEye, Inc., Form 10-Q for the Quarterly Period Ended June 30, 2021, <https://www.sec.gov/Archives/edgar/data/1370880/000137088021000033/feye-20210630.htm>, p. 12 (“The transition period is expected to be approximately 12 to 18 months after the sale closes”).

<sup>118</sup> See “Dell Technologies Announces Completion of VMware Spin-off,” Dell Technologies, November 1, 2021, <https://www.dell.com/en-us/dt/corporate/newsroom/announcements/detailpage.press-releases~usa~2021~11~20211101-dell-technologies-announces-completion-of-vmware-spin-off.htm#/filter-on/Country:en-us>. Dell acquired VMware in 2015, *i.e.*, six years before this divestiture. (See Ron Miller and Alex Wilhelm, “Dell Is Spinning Out VMware in a Deal Expected to Generate Over \$9B for the Company,” TechCrunch, April 14, 2021, <https://techcrunch.com/2021/04/14/dell-is-spinning-out-vmware-in-a-deal-expected-to-generate-over-9b-for-the-company/>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

<sup>119</sup> See Dell Technologies Inc., Form 8-K, dated October 29, 2021, <https://investors.delltechnologies.com/static-files/072b94f3-090e-4891-a825-0014a787b6c9>, p. 4 (“In connection with the Spin-Off, on November 1, 2021, Dell entered into a [...] Transition Services Agreement[.]”). See also Dell Technologies Inc., Form 10-Q for the Quarterly Period Ended October 28, 2022, <https://www.sec.gov/Archives/edgar/data/1571996/000157199622000044/dell-20221028.htm>, pp. 15, 49 (“Transition services may be provided for up to one year”).



- e. Dell EMC's 2017 divestiture of its Enterprise Content Division, valued at \$1.62 billion,<sup>120</sup> to Open Text Corporation (expected operational timeline up to over 365 days).<sup>121</sup>

51. These examples illustrate that the divestiture of integrated assets often take over 360 days even when the level of integration is expected to be relatively low, as evidenced by a divested asset that can be defined based solely on product market and/or the divestiture of a recently-acquired asset. While these examples would not be representative of the high level of integration that exists between TikTok's U.S. application and its global application (or ByteDance), they nevertheless show that divestitures are complex and time-consuming processes, which often require post-closing services from the seller to ensure business continuity. Again, these types of services would not be possible under a "qualified divestiture."

52. To be sure, when the level of integration and complexity is lower than what exists with respect to TikTok's U.S. application and its global application (or ByteDance), the operational timeline of divestitures can take fewer than 360 days. However, based on the divestitures in my sample for which I was able to identify an operational timeline, these still take well over 270 days. In case of all three divestitures below, the divested asset was defined based

---

<sup>120</sup> See "OpenText Signs Definitive Agreement to Acquire Dell EMC's Enterprise Content Division, including Documentum," PR Newswire, September 12, 2016, <https://www.prnewswire.com/news-releases/opentext-signs-definitive-agreement-to-acquire-dell-emcs-enterprise-content-division-including-documentum-300326059.html>. Dell acquired EMC in 2016, *i.e.*, the year of this divestiture. (See Noreen Seebacher, "OpenText Acquires Dell EMC's Enterprise Content Division, Including Documentum," CMSWire, September 12, 2016, <https://www.cmswire.com/information-management/opentext-acquires-dell-emcs-enterprise-content-division-including-documentum/>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

<sup>121</sup> See Dell Technologies Inc., Form 10-K for the Fiscal Year Ended February 2, 2018, <https://investors.delltechnologies.com/static-files/9d4aca86-7fd6-4b4f-ab4b-4895fa562826>, p. 104 ("Transition services may be provided for up to one year, with an option to renew after that period").

solely on product market (*i.e.*, they have one of the indicia of a less complex divestiture than the divestiture required of Petitioners),<sup>122</sup> and they still took well over 270 days. Specifically:

- a. The operational timeline of Citrix Systems Inc.’s 2017 divestiture of its GoTo subsidiary, valued at \$2.85 billion, to LogMeIn Inc. took 335 days.<sup>123</sup>
- b. The operational timeline of Symantec’s 2019 divestiture of its enterprise security business, valued at \$10.70 billion, to Broadcom took 330 days.<sup>124</sup>
- c. The operational timeline of Altaba Inc.’s 2017 divestiture of Yahoo!’s operating business, valued at \$4.48 billion, to Verizon took 324 days.<sup>125</sup>

<sup>122</sup> See Liana B. Baker, “LogMeIn to Merge with Citrix’s GoTo Unit in All-Stock Deal,” Yahoo Finance, July 26, 2016, <https://finance.yahoo.com/news/logmein-merge-citrixs-goto-unit-002645133.html>; “Broadcom to Acquire Symantec Enterprise Security Business for \$10.7 Billion in Cash,” Broadcom, August 8, 2019, <https://investors.broadcom.com/news-releases/news-release-details/broadcom-acquire-symantec-enterprise-security-business-107>; “Verizon Completes Yahoo Acquisition, Creating a Diverse House of 50+ Brands Under New Oath Subsidiary,” Verizon, June 13, 2017, <https://www.verizon.com/about/news/verizon-completes-yahoo-acquisition-creating-diverse-house-50-brands-under-new-oath-subsiadiary>. For all three of these divestitures, the public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

<sup>123</sup> I considered the start of the operational timeline the date of the TSA, January 31, 2017. I considered the end of the operational timeline December 31, 2017, the date when the company stated that “the transition services are substantially complete.” See LogMeIn, Inc., Form 10-K for the Fiscal Year Ended December 31, 2016, <https://www.sec.gov/Archives/edgar/data/1420302/000119312517063977/d301311d10k.htm#toc>, p. 90; LogMeIn, Inc., Form 10-K for the Fiscal Year Ended December 31, 2017, <https://www.sec.gov/Archives/edgar/data/1420302/000119312518050503/d506130d10k.htm>, p. 71.

<sup>124</sup> I considered the start of the operational timeline August 8, 2019, the date of the Asset Purchase Agreement to which the TSA was attached. I conservatively considered the end of the operational timeline July 2, 2020, because the parties reported having incurred transition services costs “during the three [...] months ended October 2, 2020.” See Asset Purchase Agreement by and Between Broadcom Inc. and Symantec Corporation, dated August 8, 2019, <https://www.sec.gov/Archives/edgar/data/1730168/000119312519217369/d790567dex21.htm>; NortonLifeLock Inc., Form 10-Q for the Quarterly Period Ended October 2, 2020, <https://www.sec.gov/Archives/edgar/data/849399/000084939920000011/nlok-20201002.htm>, p. 10.

<sup>125</sup> I conservatively considered the start of the operational timeline July 25, 2016, because “the Yahoo transaction was announced” in July 2016. I considered the end of the operational timeline June 13, 2017, the date when “Oath beg[an] operation[.]” See “Verizon Completes Yahoo Acquisition, Creating a Diverse House of 50+ Brands Under New Oath Subsidiary,” Verizon, June 13, 2017, <https://www.verizon.com/about/news/verizon-completes-yahoo-acquisition-creating-diverse-house-50-brands-under-new-oath-subsiadiary> (Oath CEO “has been leading integration planning teams since the Yahoo transaction was announced in July 2016”).

53. In other words, from the 26 divestitures that satisfied the criteria described in paragraphs 42-43,<sup>126</sup> and for which I could identify the beginning and end of the operational timeline, I have found none where the operational timeline took fewer than 270 days (in fact, I have found none with an operational timeline shorter than 324 days).<sup>127,128</sup> **Figure 2** below summarizes the results of my analysis based on: (i) the three Verizon divestitures described in **Section III.D.1**, and (ii) the 26 divestitures in my market sample.

---

<sup>126</sup> *I.e.*, divestiture transactions where: (1) the divested assets operated in the following industries: “interactive media and services,” “application software,” “systems software,” or “integrated telecommunication services;” (2) the transaction (i) took place in the United States, (ii) was announced and completed in the last ten years (between 2014 and 2024), and (iii) had a total transaction value greater than \$1 billion; and (3) at least one of the buyer or the seller had publicly available SEC filings at the time of the divestiture, and the transaction was subject to regulatory or antitrust approval.

<sup>127</sup> In the case of the six remaining divestitures from this sample, I was unable to identify an operational timeline because I could not find a start date, end date, or both. All six of these divestitures have indicia of less complexity than the divestiture required of Petitioners (*i.e.*, the divested asset was defined based solely on product market and/or the seller acquired the divested asset within ten years before the divestiture). These are: (1) XO Holdings, Inc.’s 2017 divestiture of its fiber-optics network business to Verizon, (2) Bain Capital, LP’s and other entities’ 2016 divestiture of the mobile and web assets of Weather Channel LLC to IBM Corporation, (3) LiveRamp Holdings, Inc.’s 2018 divestiture of its Acxiom marketing solutions business to The Interpublic Group of Companies Inc. (4) Lumen Technologies, Inc.’s 2017 divestiture of its data centers and colocation business to BC Partners and other entities, (5) Intrado Corporation’s and Apollo Global Management, Inc.’s 2023 divestiture of its safety business to Stonepeak Partners LP, and (6) Aon plc’s 2017 sale of its “technology-enabled benefits and human resources platform” to Tempo Acquisition, LLC, Blackstone Group L.P. *See Exhibit 1.*

<sup>128</sup> As I described in footnote 17, from the day of submitting my declaration on June 20, 2024, Petitioners have only 214 days left until January 19, 2025; and they have only 304 days left until April 19, 2025.

**Figure 2 - Number of Divestitures in the TMT Sector, Grouped by Indicia of Complexity and Length of Operational Timeline<sup>129</sup>**

<b>Operational timeline</b>	<b>Highly integrated based on both indicia</b>	<b>Less integrated based on at least one indicia</b>	<b>Total</b>
<b>Over 360 days</b>	7	13	<b>20</b>
<b>Under 360 days but over 270 days</b>	0	3	<b>3</b>
<b>Under 270 days</b>	0	0	<b>0</b>
<b>Unknown length</b>	0	6	<b>6</b>
<b>Total</b>	<b>7</b>	<b>22</b>	<b>29</b>

54. This analysis is consistent with information provided by Petitioners to CFIUS, which estimates that migrating TikTok’s software, including its recommendation engine and internal tools, would take at least approximately two years.<sup>130</sup> Critically, this two-year timeline was premised on several significant operational assumptions and caveats. For instance, the timeline assumes that not all tools and processes would be migrated; for example, “Content Moderation Systems will continue to be developed in China but be subject to open source to the public,”<sup>131</sup> and there would be continued access to “internal reference code from global development.”<sup>132</sup> Additionally, this two-year timeline relates to migrating certain tools to “TikTok employees working in locations where the TikTok service is offered.”<sup>133</sup> So, even if the

<sup>129</sup> As described in footnote 95, given that operational timelines are frequently underestimated, where the available information provided a range as the expected operational timeline, I present in this table the upper end of the range (while presenting the full range in **Exhibit 1**).

<sup>130</sup> NSA Presentation, 2023, p. 16.

<sup>131</sup> NSA Presentation, 2023, p. 16.

<sup>132</sup> NSA Presentation, 2023, p. 13.

<sup>133</sup> NSA Presentation, 2023, p. 13.

two-year timeline were met, it would not sever all “operational relationships” between Petitioners and TikTok’s U.S. application.

55. Finally, I note that—although a member of Congress suggested that Kunlun’s (a Chinese video game company’s) 2020 divestiture of the Grindr application indicates that Petitioners will be able to divest TikTok’s U.S. application “quickly” and with “no disruption to users”<sup>134</sup>—there are several reasons why this comparator is incorrect. Unlike the high level of integration between TikTok’s U.S. application and its global application (or ByteDance), Grindr was not highly integrated with Kunlun before its divestiture. Therefore, the Grindr divestiture did not require untangling highly integrated assets.

- a. First, Grindr was developed as a separate business from Kunlun, and Kunlun acquired a majority share in Grindr only four years before the divestiture.<sup>135</sup>
- b. Second, the divestiture did not involve the untangling of assets within the Grindr platform, as Kunlun acquired and then divested Grindr in its entirety—in other words, Kunlun simply unwound the acquisition from four years prior.<sup>136</sup>

Accordingly, S&P Capital IQ Pro categorizes the Grindr divestiture as “M&A –

---

<sup>134</sup> “[TikTok’s] divestment requirement is not new. It is not without precedent. When the app Grindr [...] was acquired by a Chinese company [...the U.S. Government...] required divestment. This happened quickly. Why? Because Grindr was a very valuable social media company. The same is true with regard to TikTok. There will be no disruption to users, just as there was [no disruption] with Grindr.” See “House Debate on H.R. 7521, H1163-1171,” Congressional Record — House, March 13, 2024, <https://www.congress.gov/118/crec/2024/03/13/170/45/CREC-2024-03-13-pt1-PgH1163-2.pdf> (Rep. Krishnamoorthi, at H1165).

<sup>135</sup> See Yuan Yang and James Fontanella-Khan, “Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns,” Los Angeles Times, March 6, 2020, <https://web.archive.org/web/20200403002228/https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns>.

<sup>136</sup> See Yuan Yang and James Fontanella-Khan, “Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns,” Los Angeles Times, March 6, 2020, <https://web.archive.org/web/20200403002228/https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns>.

Whole,” indicating that this transaction involved the sale of a whole legal entity, rather than the divestiture of a subset of assets within the company that needed to be untangled and separated.<sup>137</sup>

- c. Third, the fact that the Grindr divestiture did not require untangling highly integrated assets is also evidenced by Kunlun’s planned 2018 IPO of Grindr,<sup>138</sup> suggesting that Grindr was easily separable from the rest of Kunlun already as of 2018.
- d. Finally, even though Grindr was substantially less integrated with Kunlun than TikTok’s U.S. application and its global application (or ByteDance), CFIUS still provided Kunlun with more time to divest Grindr than what the Act affords to Petitioners. Specifically, the CFIUS NSA (signed on May 9, 2019) provided Kunlun with 419 days to divest.<sup>139</sup> In fact, Kunlun and the buyer did not sign an “Amended and Restated Stock Purchase Agreement” until May 13, 2020 (*i.e.*, 371 days after the execution of the NSA), showing that even this less complex divestiture was not completed within 360 days.

---

<sup>137</sup> This is the reason why the Grindr divestiture was not part of the 26 TMT divestitures I analyzed. As described in footnote 70, to identify divestiture transactions in S&P Capital IQ Pro, I used the filter “Transaction Type” to select transactions that were either “M&A - Asset” or “M&A - Spinoff or Splitoff.”

<sup>138</sup> See “Grindr: Chinese Parent Company Plans to List Gay Dating App,” BBC, July 30, 2019, <https://www.bbc.com/news/business-49160406>.

<sup>139</sup> The NSA was signed with CFIUS on May 9, 2019, and it ordered Kunlun to divest Grindr by June 30, 2020. See Trade Practitioner, “CFIUS Mitigation: Beijing Kunlun Wanwei Technology Co. and Grindr Inc.,” Squire Patton Boggs, June 19, 2019, <https://www.tradepractitioner.com/2019/06/cfius-beijing-kunlun-wanwei-technology-grindr/>.

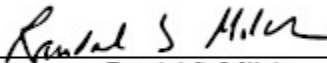
**E. A “qualified divestiture” of TikTok’s U.S. application is not operationally feasible within the timeline required by the Act**

56. As I showed in **Section III.C**, TikTok’s U.S. application is highly integrated with the global TikTok application (and with ByteDance). Additionally, as I showed in **Section III.D**, the operational timeline alone (*i.e.*, not considering the corporate timeline) of complex divestitures of highly integrated technical assets consistently takes over 360 days and necessitates post-closing support from the seller. Furthermore, the operational timeline of even less integrated assets also often takes over 360 days, and I have found no examples from the 26 divestitures in my market sample where the operational timeline took fewer than 270 days.

57. Therefore, the available information and my experience with complex divestitures support my opinion that a “qualified divestiture” of TikTok’s U.S. application is not operationally feasible within 360 days (let alone within 270 days).

\*\*\*

Pursuant to 28 U.S.C § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on June 17, 2024.

  
\_\_\_\_\_  
Randal S. Milch





participation on the Committee on Foreign Investment in the United States (“CFIUS”). I was promoted to Senior Counsel within DOJ’s Criminal Division and then National Security Division, which was created during my tenure. I was responsible for coordinating DOJ’s (including FBI’s) participation in the CFIUS process and directly advised the Attorney General and Deputy Attorney General on CFIUS matters.

3. As DOJ’s lead on CFIUS, I reviewed over 200 transactions. I was the lead negotiator on behalf of CFIUS for most of the prominent transactions reviewed from 2004-2007. I authored multiple requests to the President to exercise executive authority to block transactions. I was the primary architect and drafter of multiple complex national security mitigation agreements and worked with the FBI and other CFIUS agencies such as the Department of Defense, the Department of Homeland Security, and Intelligence Community agencies to assess national risks and to develop mitigation strategies. Most of the complex CFIUS matters I handled involved transactions with technology companies, including in sectors such as telecommunications, cloud computing, semiconductor design, data center technology, and computer software. I led CFIUS mitigation negotiations that were among the first to include complex physical and logical access restrictions to technology platforms and reliance upon source code review as means of discovering and deterring attacks by nation-states.

4. Since 2008, I have been a national security consultant and lawyer and simultaneously have started multiple companies, including Corsha, Inc., a successful technology company that offers a patented cybersecurity solution for machine-to-machine network traffic that I was involved in designing and developing. From 2011 to 2017, I was the CEO and Co-Founder of Chain Security, LLC, a professional services firm. Our clients were primarily technology companies who were selling computing equipment and software, including

cybersecurity software, to the U.S. Government and U.S. critical infrastructure. Our customers typically hired us to help analyze and solve concerns raised by government customers concerning technology supply chains as well as research, development, and production being performed outside the U.S., most often in China. As a consultant, I advise large corporations, technology companies, and defense contractors on national security matters, including CFIUS transactions, as well as operations and processes required to protect sensitive information. I currently serve as a technology and security advisor for a biotech company, and I am also currently an advisor to two different companies in the national security space where one of my roles is to assess commercial technology platforms for repurposing as national security platforms. I also serve as a consultant and expert to law firms handling CFIUS transactions. I have led efforts to analyze national security vulnerabilities and to put in place operational and technical mitigation plans that were presented to government customers, including tracing the origins of software and hardware components and maintaining secure chains of custody for software. I remain abreast of current CFIUS trends and approaches to mitigation as well as how U.S. Government agencies with defense, intelligence, and law enforcement responsibilities assess risks associated with the security of data and information systems, particularly with respect to China. I have been a testifying expert in CFIUS-related litigation. A copy of my curriculum vitae is attached hereto as Appendix 1.

**SUMMARY OF DECLARATION**

5. Through their counsel, I have been retained by Petitioners TikTok Inc. and ByteDance Ltd. (“Petitioners”)<sup>1</sup> to analyze the draft National Security Agreement, dated August

---

<sup>1</sup> References to ByteDance are to the corporate group as opposed to any particular corporate entity. However, such references exclude TikTok U.S. Data Security Inc. (“TTUSDS”), as discussed *infra* paras. 39, 46-50, 53.

23, 2022, between these parties and CFIUS (“NSA”), and to offer an opinion on whether the NSA as drafted would mitigate the national security concerns expressed by sponsors of the Protecting Americans From Foreign Adversary Controlled Applications Act (the “Act”) which coincide with the rationale expressed by CFIUS during its TikTok review.

6. Throughout this Declaration, I will use the term “TikTok U.S. App” or simply the “App” to mean collectively the TikTok mobile app and the web-based version of TikTok that specifically are used by a “TikTok U.S. User.”<sup>2</sup> A “TikTok U.S. User” or “User” is a person using the App who is (i) in the U.S., or (ii) outside the U.S. but is identifiable as a U.S. person.<sup>3</sup> I will use the term “TikTok U.S. Platform” or simply the “Platform” to mean the platform components (as explained more fully below) that specifically support the TikTok U.S. App.<sup>4</sup>

7. The U.S. Government, including Congress and CFIUS, use a widely adopted model for assessing national security risks. The risk model has multiple components—threat, vulnerability, and consequences. Using an analytic approach to each component enables decision makers to understand what mitigation may be required to lower national security risk to acceptable levels.

8. CFIUS and Petitioners engaged in protracted and detailed mitigation negotiations over the course of nearly two years, culminating in the NSA. I have reviewed the NSA. Using the risk model, my professional opinion is that if implemented as written, the NSA would effectively mitigate the U.S. national security risks associated with Petitioners owning and deploying the TikTok U.S. App and TikTok U.S. Platform.

---

<sup>2</sup> See NSA Sec. 1.33.

<sup>3</sup> See NSA Sec. 1.35.

<sup>4</sup> See NSA Sec. 1.34.

9. I have organized this Declaration into the following sections, with references to the corresponding paragraphs:

- A. METHODOLOGY (paras. 10-29), which includes these subsections:
  - i. Overview of the Risk Model (paras. 11-17)
  - ii. Threat (para. 18)
  - iii. Vulnerability/Consequences (paras. 19-22)
  - iv. The Role of Mitigation (paras. 23-29)
- B. ANALYSIS (paras. 30-104), which includes these subsections:
  - i. History of Negotiations (paras. 32-37)
  - ii. Key Elements of the NSA (paras. 38-75)
  - iii. Caveats and Assumptions (paras. 76-80)
  - iv. Analysis of the NSA (paras. 81-104)
- C. CONCLUSIONS (paras. 105-107)

**METHODOLOGY**

10. To assess the NSA, I will use the established risk-based methodology that is well-known and well-accepted across the government’s national security community. First, I will frame the model’s importance in national security decision making and summarize how the model works. I will then discuss in more depth each of the components or parameters that feed into the risk model. I will then discuss the role of mitigation in addressing national security risk.

***Overview of the Risk Model***

11. It is important to understand the reasons for using a model for analyzing national security risk, rather than falling back on broad or vague national “interests” tests when making national security decisions. By relying on an analytic model with specific parameters, the U.S.

Government is empowered to make better decisions about when to take action to protect national security interests and what actions to take. The model ensures that Congress, CFIUS, and other government decision makers are more rigorous in assessing which specific mitigation mechanisms are needed to protect national security, how those mechanisms should be implemented and by whom, and how to measure their effectiveness. The model is intended to blunt the temptation to substitute political decisions or “gut feelings” for analysis in situations where, either by long-standing consensus or as mandated by law, a more precise, thoughtful, and thorough national security determination is required.

12. U.S. Government agencies use this risk model when assessing cybersecurity risks and other national security risks to networks, data, privacy, and information systems.<sup>5</sup> For example, as recently as March 2024, the Government Accountability Office relied on this risk model when advising Congress on cybersecurity risks to critical infrastructure systems.<sup>6</sup> In 2018, Congress codified this risk model in the statute that governs CFIUS, requiring CFIUS to use the model when deciding whether to allow, block, or mitigate transactions under review.<sup>7</sup> CFIUS has likewise codified this risk model in its regulations.<sup>8</sup>

---

<sup>5</sup> See, e.g., Nat’l Counterintelligence and Sec. Ctr., Off. of Dir. of Nat’l Intel., *Framework for Assessing Risks* (April 2021), [https://www.dni.gov/files/NCSC/documents/supplychain/Framework\\_for\\_Assessing\\_Risks\\_-\\_FINAL\\_Doc.pdf](https://www.dni.gov/files/NCSC/documents/supplychain/Framework_for_Assessing_Risks_-_FINAL_Doc.pdf) [hereinafter “ODNI Framework”]; Nat’l Inst. of Standards & Tech., Dep’t of Com., NIST Special Pub. 800-30 Rev. 1, *Guide for Conducting Risk Assessments* (Sept. 2012), <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>; Dep’t of Homeland Sec., *DHS Risk Lexicon* (Sept. 2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf> [hereinafter “DHS Lexicon”].

<sup>6</sup> See U.S. Gov’t Accountability Off., *Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology* (Mar. 2024), <https://www.gao.gov/assets/gao-24-106576.pdf>.

<sup>7</sup> See Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. 115-232, 132 Stat. 2174 (2018) (codified at 50 U.S.C. § 4565).

<sup>8</sup> See 31 C.F.R. § 800.102 (Risk-based analysis).

13. In the lexicon of this model, “risk” is a term of art. The simplified formula for risk is as follows: Risk = Threat \* Vulnerability/Consequences. Because each of these elements – threat and vulnerability/consequences– are qualitative rather than quantitative, the formula is obviously not intended to be mathematical. Instead, it represents a qualitative combination of each element to make a holistic determination about national security interests.

14. When conducting an analysis using the model, a decision maker or analyst considers each of the elements independently using data that is specific to the element. Each element is then typically scored as low, medium, or high. The elements are then combined or “averaged” to produce an overall risk that is either low, medium, or high. For example, in a given national security context, such as an acquisition of a U.S. company by a non-U.S. buyer, the model could indicate that the THREAT is LOW and the VULNERABILITY/CONSEQUENCES is HIGH, leading to a conclusion that the overall RISK to national security for the transaction is HIGH. Similarly, e.g., the model could indicate that the THREAT is HIGH, but the VULNERABILITY/ CONSEQUENCES are LOW, giving the transaction an overall risk of LOW.

15. Again, the formula is ultimately qualitative, so it is not as simple as saying, e.g., two LOWs and a HIGH average out to a MEDIUM. Some judgment and weighting are required, depending on the context. The qualitative risk scoring guides the analysis and suggests roughly the overall risk outcome.

16. In my experience in the CFIUS context, when the model indicates that the national security risk for a transaction is HIGH, CFIUS typically either (i) has demanded that the parties agree to mitigation or (ii), in cases where mitigation was not sufficient or if the parties would not agree to CFIUS’s demands, has recommended that the President exercise his authority

to block the transaction or requested the parties to abandon the transaction. For transactions that are rated as a MEDIUM risk, CFIUS has typically required some level of mitigation, but has rarely blocked such transactions. Transactions with LOW risk are typically approved without further action.

17. When assessing any of the model's components, U.S. Government decision makers typically rely on a mix of publicly available information, unclassified but confidential government information, and classified information. Congress and CFIUS can draw on reporting from the U.S. intelligence, defense, and law enforcement communities, particularly for threat information, as well as on expertise across the government for sensitive information about threats, vulnerabilities, and consequences. Parties to a transaction, such as the Petitioners, are also very important sources of information, particularly related to vulnerabilities. Government agencies also use a review of open-source information to understand technologies, industry dynamics, and customer use cases.

### ***Threat***

18. Under the lexicon of the risk model, "threat" focuses on an assessment of the foreign or non-U.S. actors in the context. For example, the threat analysis here would be focused on ByteDance and, because it is indirectly wholly owned by ByteDance Ltd., TikTok Inc. The specific question when assessing a threat is whether the foreign person at issue has (a) an intent and (b) a capability to take action that would impair U.S. national security.<sup>9</sup> As discussed below, I assume for purposes of this Declaration, that the U.S. Government will consider the Chinese

---

<sup>9</sup> See, e.g., 31 C.F.R. § 800.102(a) (CFIUS definition of "threat"); see also ODNI Framework, *supra* note 5, at 2 ("From the threat perspective, an understanding of the adversary's intentions and capabilities is vital. Key to this is using the latest threat information to determine if specific and credible evidence suggests an item or service might be targeted by adversaries.").



government and most if not all Chinese companies as posing a HIGH threat to U.S. national security interests.

*Vulnerability/Consequences*

19. The “vulnerability” and consequences analyses are focused on the U.S. company, U.S. person, or U.S.-based assets in the transaction. The analysis can consider an entire U.S. business or just U.S.-based assets, data, or operations in the business.

20. The vulnerability analysis for the current context would be focused on the TikTok U.S. App and the TikTok U.S. Platform. The specific question when assessing a vulnerability is whether the U.S. company, person, or assets could be exploited by the foreign person (i.e., the foreign “threat” actor) to hurt or impair U.S. national security.<sup>10</sup>

21. Sponsors of the Act identified two U.S. interests that could be harmed by the Petitioners through their control of the TikTok U.S. App and the TikTok U.S. Platform.<sup>11</sup> The first is the data about U.S. users or subgroups of users that is gathered by or stored on the TikTok U.S. Platform as a result of using the TikTok U.S. App. The data could include personal identifying information, financial information, geolocation, social connections, and patterns of

---

<sup>10</sup> See, e.g., 31 C.F.R. § 800.102(b) (CFIUS definition of “vulnerability”); see also DHS Lexicon, *supra* note 5, at 38 (“physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard”).

<sup>11</sup> While I have limited my discussion in this Declaration to the two asserted vulnerabilities that apparently motivated the sponsors of the Act, as part of my analysis I considered an expanded array of relevant national security vulnerabilities, including those cited by CFIUS. See, e.g., Exec. Order No. 14083, Sec. 3(c)(i), 87 Fed. Reg. 57369, 57372-73 (Sept. 15, 2022); Letter from Thomas P. Feddo, Assistant Secretary Investment Security, U.S. Dept. of Treasury (on behalf of CFIUS) to David N. Fagan and Michael E. Leiter (counsel for ByteDance and TikTok) 3 (Jul. 30, 2020) (CFIUS referral to the President). My opinion that the NSA would effectively mitigate national security risks includes mitigating the full array of vulnerabilities I considered that could possibly be associated with the TikTok U.S. App and the TikTok U.S. Platform.

behavior. Whether standing alone or combined with other compromised data sets, compromised user data could be used for “the surveillance, tracing, tracking, and targeting of individuals or groups of individuals,” particularly in light of recent advancements in artificial intelligence and data science.<sup>12</sup> The second interest identified by congressional sponsors of the Act is that the content on the TikTok U.S. Platform could be manipulated to serve the interests of the Chinese government through spreading pro-Chinese propaganda, censoring anti-Chinese content, or promoting content intended to incite disunity and foment hate in the U.S. on divisive issues.

22. The “consequences” (sometimes called “impact”) assessment is closely related to the vulnerability assessment and is often included as an element of vulnerability. The consequences assessment focuses on the specific national security interests at stake or affected by the U.S. company, person, or asset. It seeks to characterize how much damage would be caused to national security if a vulnerability is exploited.

***The Role of Mitigation***

23. The role of mitigation is to reduce specific elements of the risk model such that the overall national security risk level drops to an acceptable level, typically LOW or MEDIUM. To accomplish this, mitigation must be specifically tuned to the elements of threat and vulnerability, including consequences.

24. Mitigation is typically accomplished by imposing a legal obligation on the parties in a particular national security context to take action to mitigate the risk. These legal obligations typically take the form of an agreement with the U.S. Government, or they may include unilateral action taken by private parties. In the context of business operations and

---

<sup>12</sup> Exec. Order 14083, Sec. 3(c)(i), 87 Fed. Reg. at 57372-73.

mergers and acquisitions, the mitigation obligations can be required of a foreign actor, a U.S. actor, or both. The NSA is an example of such a mitigation contract.

25. The U.S. Government has a long history of favoring mitigation to reduce national security risks. CFIUS is a prime, but not exclusive, example of a government entity engaging in mitigation to reduce risk. The Federal Communications Commission (“FCC”), in conjunction with the interagency group “Team Telecom,”<sup>13</sup> adopts mitigation agreements similar to those imposed by CFIUS as a condition of granting Section 214 licenses to non-U.S. applicants for the provision of international telecommunications services to or from the United States. The U.S. Department of Defense as well as Intelligence Community agencies frequently enter into mitigation agreements to address foreign ownership, control, and influence by foreign persons over U.S. companies and will also enter into agreements or require unilateral action to reduce risk in technology supply chains.

26. CFIUS has been reluctant to use mitigation to lower national security risk when the mitigation depends on an untrusted foreign company to faithfully implement the mitigation terms. CFIUS has reasoned that, e.g., it cannot trust a Chinese company to comply with contractual mitigation commitments if the Chinese government at some point demands that the company take action against U.S. national security interests. This is the reason many China-related transactions have been turned away by CFIUS in recent years, when similar transactions deriving from other high-threat countries have been cleared subject to mitigation.

27. The exception to this pattern is when CFIUS has been able to rely on a trusted third-party U.S. company as the primary mechanism for ensuring compliance with mitigation, even in China-related transactions. In such cases CFIUS has been able to get comfortable with

---

<sup>13</sup> See Exec. Order 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020).

entering into mitigation agreements similar to the NSA. Under the rubric of the risk model, the reliance on a trusted third party helps reduce the foreign party's access to U.S. national security assets and thereby effectively reduces the ability of the foreign party to exploit vulnerabilities.

28. A public example of this is the CFIUS approval in 2018 of the proposed acquisition of Genworth Financial, a U.S. mortgage insurance provider, by China Oceanwide Holdings. CFIUS's approval was conditioned on the use of "a U.S.-based, third-party service provider to manage and protect the personal data of Genworth's U.S. policyholders" after the transaction closed.<sup>14</sup> Another public example is Lenovo's acquisition of IBM's PC Division in 2005 and its subsequent acquisition of IBM's X86 server business in 2014.<sup>15</sup> CFIUS approved both transactions subject to mitigation agreements that required IBM to continue playing a primary role in servicing the computing equipment for years after the transaction closed, despite no longer owning the sold assets. CFIUS was able to rely on IBM's bona fides to ensure that the key technical and process-related terms of the mitigation were faithfully and effectively implemented, without having to rely on Lenovo, which at the time was a Chinese company with Chinese government ownership.

29. In addition to using a trusted U.S. third party to lower the vulnerability level, mitigation agreements used by not only CFIUS but other government agencies have relied on a

---

<sup>14</sup> See *Genworth Financial Announces Second Quarter 2018 Results*, Genworth (Jul. 31, 2018) <https://investor.genworth.com/sec-filings/all-sec-filings/content/0001193125-18-233445/d610764dex991.htm>.

<sup>15</sup> See, e.g., Patrick Moorhead, *IBM-Lenovo Server Agreement Basically a Done Deal*, Forbes (Aug. 26, 2014) <https://www.forbes.com/sites/patrickmoorhead/2014/08/26/ibm-lenovo-server-agreement-basically-a-done-deal/?sh=aa570a24bbc7>; *Committee on Foreign Investment in U.S. Completes Review of Lenovo-IBM Deal*, Lenovo (Mar. 9, 2005) <https://news.lenovo.com/pressroom/press-releases/committee-on-foreign-investment-in-u-s-completes-review-of-lenovo-ibm-deal/>.

number of well-accepted mitigation principles, primarily aimed at reducing vulnerabilities. They include (i) technical and operational processes that eliminate or materially reduce access to products and services, with a goal of reducing the level of access available to a foreign “threat” actor to exploit vulnerabilities; (ii) mechanisms for high visibility and accountability through inspections, auditing, and monitoring, with the goal of deterring a foreign “threat” actor from taking adverse action that would be discovered and could lead to significant criminal penalties or unilateral action by U.S. law enforcement, defense, and/or intelligence agencies; (iii) automatic and in some cases liquidated damages provisions and other enforcement and penalty mechanisms for non-compliance, with the goal of deterring exploitation with a threat of significant monetary penalties; and (iv) provisions allowing for CFIUS to reopen reviews or unilaterally initiate stoppages or even divestment for material non-compliance, which preserves CFIUS’s power to take additional action to protect national security for the entire term of a mitigation agreement.

**ANALYSIS**

30. The purpose of this Declaration is to analyze the NSA as written and offer an opinion, based on my professional experience, as to whether it is sufficient to mitigate national security risk to a level that should be acceptable to Congress and CFIUS.

31. I believe it is important to contextualize the NSA. Based on my experience negotiating other such agreements, the NSA was likely the result of thousands of collective hours of work between CFIUS, the Petitioners, and their advisors to arrive at the best possible solution to address national security risk in the context of the TikTok U.S. App and the TikTok U.S. Platform. I therefore will summarize the history of negotiations surrounding the NSA. I will then provide an overview description of the key terms of the NSA as well as an explanation of important caveats and assumptions that are relevant to my analysis. I will then analyze the terms

of the NSA itself using the risk model I have described above and will draw conclusions about the effectiveness of the NSA's terms to mitigate national security risk.

*History of Negotiations*

32. Petitioners formally filed a voluntary notice with CFIUS on May 27, 2020. A first period of engagement resulted in CFIUS referring the matter to President Trump on July 30, 2020, and President Trump issuing a divestment order on August 14, 2020.

33. I understand that Petitioners and the U.S. Government agreed to an abeyance of the litigation Petitioners brought challenging the divestment order so they could engage in negotiations to determine whether mitigation was possible.

34. After exchanging terms sheets, Petitioners provided CFIUS with a first draft of the NSA on January 4, 2021. From January 2021 through August 2022, Petitioners and CFIUS engaged in active negotiations regarding the terms of the NSA. Based on the CFIUS record, at least 23 sets of revisions to the NSA were exchanged between the parties. In that time period, CFIUS heavily redlined all or a portion of the NSA eight different times. Many of CFIUS's revisions or comments reflect that the Committee and its agencies very actively tried to understand the TikTok U.S. App and platform and how they would operate at a technical level. The substantive provisions of the NSA that CFIUS commented on or revised ranged from corporate governance, U.S. control of TikTok U.S. Data Security Inc. ("TTUSDS"), hiring by TTUSDS, the role of the Trusted Technology Partner,<sup>16</sup> use of technical vendors and contractors, mechanisms for source code review, chain of custody for reviewed code, storage and protection of "Protected Data," monitoring, auditing, and enforcement. Petitioners' responses appear to incorporate or accept with some revision the vast majority of revisions proposed by CFIUS.

---

<sup>16</sup> As discussed *infra* paras. 54-56.

35. In addition to written redline exchanges, the CFIUS record indicates that between January 2021 and August 2022, there were at least 14 meetings or calls between CFIUS and Petitioners to discuss NSA terms. The meetings included at least nine written presentations by Petitioners to CFIUS about the NSA mitigation mechanisms and the status of implementation. In addition to meetings and presentations, there were at least 15 additional email exchanges where CFIUS posed questions related to Petitioners' operations and the NSA terms, which emails were followed by written responses by Petitioners.

36. In short, CFIUS and Petitioners had a protracted, detailed, and productive negotiation over nearly two years that led to the version of the NSA at issue here.

37. The final working draft of the NSA was delivered by Petitioners to CFIUS on August 23, 2022. Including its annexes, the NSA is 103 pages long and is the most sophisticated and thorough mitigation agreement I have reviewed in my 20 years of working on national security agreements, including my time as a member of CFIUS and in my current legal and consulting roles advising companies in their negotiations with CFIUS as well as with the Department of Defense and the Intelligence Community.

***Key Elements of the NSA***

38. The NSA is lengthy and has a significant amount of detail about the overarching mitigation mechanisms. I will not recount all of the details, but to inform my analysis of the terms, I provide here an overview description of the key terms of the NSA that I believe are most relevant to my analysis and conclusions. I will define a few key terms that are important to understanding the NSA. I am using definitions in a more colloquial way than the precise

contractual language in the NSA. The precise definitions of these terms will of course still be informed by the NSA itself.<sup>17</sup>

39. The NSA requires the creation of a new entity called TTUSDS. It is to be a U.S. corporation and a wholly owned subsidiary of TikTok Inc. The role of TTUSDS is critical to the NSA.<sup>18</sup>

40. Non-public personal information about TikTok U.S. Users, whether it is provided to the App by the User or gathered from use of the App, is defined as “Protected Data.”<sup>19</sup> It is this Protected Data that is central to one of the two national security risks raised by sponsors of the Act—i.e., intelligence collection. The App and Platform contain other information, such as user content, that is meant to be shared as well as information from other platforms or data sets that is non-confidential such as news and advertisements, all of which is considered to be publicly available and is defined as “Public Data” in the NSA.<sup>20</sup>

41. The Platform includes various layers of software, including software referred to as the “Recommendation Engine,” which continuously learns from User behavior as well as input from TikTok Inc. to recommend content to TikTok U.S. Users.<sup>21</sup> This Recommendation Engine is central to the second national security risk raised by sponsors of the Act—i.e., propaganda.

42. When software developers or engineers write computer software, they use words and phrases that describe the logic and commands of the software. There are different coding

---

<sup>17</sup> I understand that Petitioners may have voluntarily started implementing some of the NSA’s terms. In this Declaration, I will discuss the NSA as if it remains completely prospective.

<sup>18</sup> See NSA Sec. 2.1.

<sup>19</sup> See NSA Sec. 1.22.

<sup>20</sup> See NSA Sec. 1.23.

<sup>21</sup> See NSA Sec. 1.24.



languages that have different ways of phrasing commands and different syntax, but ultimately all coding languages are readable to a human. This human-readable set of commands is called “Source Code.”<sup>22</sup> A trained engineer who understands the general function of software and who knows the particular coding language that was used should be able to read Source Code, understand what the software will do and how it will operate, and spot anomalies and vulnerabilities. There are also automated tools available that can read Source Code to ensure integrity and spot vulnerabilities. Source Code reviewers often use these automated tools to assist with manual reviews.

43. To deploy software to a machine or a computer and make it work as an application, Source Code must be converted from words and phrases to “binary” code, which consists of 1s and 0s. This conversion is done through feeding Source Code into a specialized set of applications in a process that is called a “Build.” The output of a Build process that has converted Source Code into a machine-executable application consisting of 1s and 0s is called “Executable Code” (sometimes also called “Object Code” or “Binary”).<sup>23</sup> Humans cannot read or understand Executable Code. There are some specialized applications that can check the integrity of Executable Code and can monitor its behavior when running as a software application. However, identifying vulnerabilities or malicious code is much easier during a Source Code review than when testing Executable Code.

44. During a Build process, the final software can consist of proprietary Source Code developed by a company as well as third party code that may be incorporated into the software. Third party code can be integrated either as Source Code or may be licensed or acquired only in

---

<sup>22</sup> See NSA Sec. 1.28.

<sup>23</sup> See NSA Sec. 1.12.

Binary form. A Build process can combine third-party Executable Code with proprietary Source Code to make a unified software application in a single final Executable form.

45. The App and the Platform are largely composed of software developed by ByteDance and its affiliates. The software is developed as Source Code, which is then run through a Build process to create Executable Code. The Executable Code for the App is published to app stores (e.g., Apple and Google) or loaded onto the TikTok website. The Executable Code for the Platform is deployed to cloud infrastructure, servers, networks, gateways, and databases in order to operate the Platform. The key functionality of the Platform is embedded in software, although that software runs on some physical infrastructure. The manner in which the App and the Platform operates as software depends on both the commands and features in the Code as well as how the App and the Platform are configured when they are installed on phones, computers, cloud infrastructure, servers, networks, and databases.

46. Under the NSA, the overall function of the newly created TTUSDS is to have primary responsibility for the security of the App and the Platform and for the protection of Protected Data. The NSA contains key provisions that directly affect the governance and control of TTUSDS and the access Petitioners have to TTUSDS and the App, the Platform, and Protected Data.<sup>24</sup>

47. The NSA requires Petitioners to relinquish both governance control and operational control over TTUSDS.<sup>25</sup> TTUSDS's Board of Directors will consist of three Security Directors who are U.S. citizens residing in the U.S. and who have had no previous

---

<sup>24</sup> See NSA Sec. 2.4.

<sup>25</sup> See NSA Sec. 2.7.

affiliation with Petitioners and who must be approved by the U.S. Government.<sup>26</sup> One of the three directors will serve as Chair. There may be other members and observers on the Board, but they can only be persons associated with TTUSDS. No representative of Petitioners can attend or participate with the TTUSDS Board unless the U.S. Government grants express approval. The exception is that TTUSDS will not be able to take certain extraordinary actions without consulting Petitioners, such as selling TTUSDS's assets or filing for bankruptcy. This allowance of Petitioners to have a say in extraordinary action is a standard provision in mitigation agreements, both with CFIUS and when the Department of Defense is mitigating foreign ownership, control, or influence of foreign-owned U.S. companies that perform classified work.

48. The management of TTUSDS will be appointed by the TTUSDS Board, and the key management personnel must all be U.S. citizens with no prior affiliation with Petitioners.<sup>27</sup> The only involvement from Petitioners is that TikTok Inc. must be consulted in setting the compensation for TTUSDS's key management personnel.<sup>28</sup>

49. The NSA also requires a change in the Board of TikTok Inc. The Board will have five members—two representing ByteDance; two outside directors who have had no prior affiliation with Petitioners and who are citizens of the U.S. or one of the “Five Eyes” countries (i.e., Canada, U.K., Australia, and New Zealand); and the Chair of TTUSDS.<sup>29</sup> TikTok Inc. must have a Compliance Officer, and TTUSDS must have a Security Officer, who are U.S.

---

<sup>26</sup> See NSA Secs. 3.1-3.2.

<sup>27</sup> See NSA Sec. 5.1.

<sup>28</sup> See NSA Sec. 3.11(3).

<sup>29</sup> See NSA Sec. 4.1.

citizens to be liaisons with TTUSDS as well as with the U.S. Government on compliance and security matters.<sup>30</sup>

50. Operationally, TTUSDS must be completely separated from Petitioners, with no sharing of locations, systems, networks, or personnel.<sup>31</sup> TTUSDS will have full autonomy, subject to oversight by the Security Directors and Third-Party Monitor, as described below, over its employees and vendors, with no input or involvement from Petitioners.<sup>32</sup>

51. The NSA allows TikTok Inc. to continue managing the business strategy in the U.S. for the App and the Platform and to coordinate that strategy with the rest of the world, which includes identifying new features, gathering customer feedback in the U.S., coordinating with advertisers, and managing certain legal, compliance, and safety matters.<sup>33</sup>

52. The Source Code for the App and the Platform will continue to be written primarily by ByteDance, presumably in China.

53. The primary thrust of the NSA is that it sets up key technical and operational security provisions that govern use of the App and the Platform, as well as access to and storage of Protected Data, and places responsibility for all of those activities exclusively in TTUSDS. The NSA refers to these as “CFIUS Functions.” They include: (i) storage and protection of Protected Data, (ii) review and inspection of all Source Code for the App and the Platform prior to the Build process, (iii) actual deployment in the U.S. of all Executable Code for the App and the Platform, (iv) all business and compliance functions that may require access to Protected

---

<sup>30</sup> See NSA Secs. 6.2, 6.3.

<sup>31</sup> See NSA Secs. 2.2, 2.5, 2.6, 2.7, 12.1(3).

<sup>32</sup> See NSA Secs. 13.1-13.7.

<sup>33</sup> See NSA Sec. 4.2.

Data, (v) review and control over the performance of the Recommendation Engine, and (vi) overall compliance with the NSA.<sup>34</sup> The NSA requires Petitioners to grant to TTUSDS all of the rights and licenses to the App and the Platform necessary to use them in the U.S.

54. A critical element in the NSA is the appointment of a Trusted Technology Partner (“TTP”) to support TTUSDS in all of these “CFIUS Functions.”<sup>35</sup> The U.S. Government must approve the appointment of the TTP. The NSA identifies Oracle, Inc., a publicly traded U.S. company, as the initial TTP. Oracle may be replaced by another approved third-party vendor if needed.<sup>36</sup>

55. The NSA requires that Petitioners and TTUSDS enter into a master services agreement with Oracle to implement the NSA.<sup>37</sup> While Petitioners are responsible for funding the efforts by Oracle, Oracle works solely under the direction of TTUSDS, and its fiduciary obligations are to TTUSDS and the U.S. Government, not to Petitioners. For all the work related to the NSA, Oracle is required to follow the same hiring parameters that govern TTUSDS—i.e., using only individuals who do not work for or have any other affiliation with Petitioners, and with constraints on the hiring of citizens of certain countries, including China.<sup>38</sup>

56. Oracle’s role is central to the entire mitigation mechanism under the NSA. Oracle will be charged with carrying out the technical aspects of TTUSDS’s obligations to secure the

---

<sup>34</sup> See NSA Sec. 2.4.

<sup>35</sup> See NSA Secs. 1.37, 2.4, 2.5.

<sup>36</sup> See NSA Sec. 1.37.

<sup>37</sup> See NSA Sec. 8.2.

<sup>38</sup> See NSA Secs. 1.4, 5.3, 8.2.

App, the Platform, and the Protected Data.<sup>39</sup> Oracle will work with other U.S.-based third-party vendors who will play additional roles for TTUSDS, as described below.

57. The NSA’s technical mitigation scheme can be understood by examining the process governing the software for the App and the Platform. After ByteDance writes the Source Code for both the App and the Platform (including the Recommendation Engine), it will deliver the Source Code to a facility in the U.S. that the NSA calls a “Dedicated Transparency Center.”<sup>40</sup> This is essentially a computer environment whose sole purpose is to hold the Source Code and make it available to TTUSDS and Oracle. There may be more than one Dedicated Transparency Center, but each one must have an exact copy of any Source Code placed in any other Center (i.e., they are mirrored). ByteDance will be able to push Source Code to the Dedicated Transparency Centers but cannot “pull” any data nor have any other access to the Dedicated Transparency Centers.<sup>41</sup>

58. The Dedicated Transparency Centers must be located only in the U.S. or in one of the “Five Eyes” countries.<sup>42</sup> There must always be a Dedicated Transparency Center located within Oracle’s own proprietary secure cloud environment, which I will refer to as the “Secure Oracle Cloud.”<sup>43</sup>

59. When ByteDance delivers Source Code to the Dedicated Transparency Centers, it must also deliver a “software bill of materials” or “SBOM” along with each tranche of Source

---

<sup>39</sup> See NSA Sec. 8.2.

<sup>40</sup> See NSA Secs. 1.10, 9.2.

<sup>41</sup> See NSA Secs. 9.1, 9.3.

<sup>42</sup> See NSA Sec. 9.1.

<sup>43</sup> See NSA Sec. 9.4; see also *id.* Sec. 8.4.

Code that is lodged.<sup>44</sup> An SBOM is a detailed list or description of all the components in the Source Code and their sources (e.g., written by ByteDance, licenses from a third party, or open source), which can include individualized Source Code modules for particular features as well as any third-party Source Code or Executable Code.

60. When ByteDance delivers Source Code and an accompanying SBOM, it must electronically sign both of them.<sup>45</sup> Electronic signatures are a technical method of fingerprinting electronic information or code. There are various methods of doing it, but the essential point is that once code is signed, it is very hard to replicate or spoof the signature. It is a way of uniquely identifying a particular copy of any Source Code or Executable Code. An electronic signature remains attached to Executable Code so that it will always be possible to know from which Source Code the deployed Executable Code was derived.

61. Once Source Code is available in the Dedicated Transparency Center, the Source Code will be reviewed. The purpose of the review will be to identify any malicious code, bugs, “backdoors,” or exploits that have been written into the Source Code as well as non-malicious vulnerabilities that sometimes result from the normal code development processes.<sup>46</sup>

62. The NSA requires TTUSDS and Oracle to retain yet another U.S.-based security vendor who specializes in reviewing source code to conduct the Source Code security review within the Secure Oracle Cloud. The NSA calls this security vendor the Source Code Inspector.<sup>47</sup>

---

<sup>44</sup> See NSA Sec. 9.2.

<sup>45</sup> See NSA Sec. 9.2.

<sup>46</sup> See NSA Sec. 9.5.

<sup>47</sup> See NSA Sec. 9.11.

63. TTUSDS, Oracle, and the Source Code Inspector are charged with ensuring that there is nothing malicious in any Source Code provided by ByteDance.<sup>48</sup> This review must be conducted on every single piece of Source Code that is required to operate the entirety of what is known as “TikTok”—i.e., the App itself and all software required for the Platform, including the Recommendation Engine.<sup>49</sup> It also includes any updates, patches, or new versions of the App or the Platform. The review must be completed for any version of the App or Platform that is deployed in the U.S., and the reviewed Source Code must match the SBOM that was delivered with it.<sup>50</sup>

64. Any indication of malicious code or exploit or any deviation from the SBOM must be reported to the U.S. Government.<sup>51</sup> TTUSDS and Oracle will require ByteDance to fix any security problem identified during the Source Code review and will report the outcome to the U.S. Government.<sup>52</sup> All security fixes or revisions performed by ByteDance must go back through the Source Code review process.<sup>53</sup>

65. If ByteDance does not correct an identified security problem to the satisfaction of TTUSDS, Oracle and the U.S. Government, the NSA gives Oracle unilateral authority to suspend the use of the App and the Platform in the U.S.<sup>54</sup>

---

<sup>48</sup> See NSA Secs. 2.4, 9.5-9.13, 9.15.

<sup>49</sup> See NSA Sec. 9.7, 9.13.

<sup>50</sup> See NSA Secs. 9.7, 9.10, 9.12.

<sup>51</sup> See NSA Sec. 9.6.

<sup>52</sup> See NSA Sec. 9.10.

<sup>53</sup> See NSA Secs. 9.7, 9.10, 9.12-9.14.

<sup>54</sup> See NSA Secs. 9.14-9.15.



66. Once Oracle signs off on reviewed Source Code for the App, Oracle will build Executable Code from the secured and signed Source Code.<sup>55</sup> This will be done exclusively in the Secure Oracle Cloud.<sup>56</sup>

67. As for the Executable Code for the Platform, it is reviewed by Oracle and built and deployed by TTUSDS. The NSA requires that the Platform be deployed on and operate exclusively in the Secure Oracle Cloud.<sup>57</sup> The NSA requires TTUSDS and Oracle to ensure that the Platform connects only to Content Delivery Networks<sup>58</sup> located in the U.S. that have no affiliation with Petitioners when delivering content within the United States.<sup>59</sup>

68. Once Oracle has built secure Executable Code for the App itself, it will use the secure version to deploy the App on the website in the U.S., which will be hosted within the Secure Oracle Cloud, and to the major app stores (e.g., Apple and Google) servicing TikTok U.S. Users.<sup>60</sup> TTUSDS and Oracle will ensure that only the reviewed versions of the App are made available in the U.S. The version of the App deployed by Oracle will be configured to allow connections only to the Platform in the Secure Oracle Cloud and to no other network or platform. Any movement of content or Public Data from TikTok U.S. Users to or from the rest of the world will be routed through the Platform in the Secure Oracle Cloud before transiting to Content Delivery Networks that carry the traffic globally.<sup>61</sup> Oracle will monitor all

---

<sup>55</sup> See NSA Secs. 8.4, 9.10, 9.12.

<sup>56</sup> See *id.*

<sup>57</sup> See NSA Secs. 8.4, 8.5, 11.5.

<sup>58</sup> Content Delivery Networks are servers and related infrastructure that are used for the delivery of static and live content to the TikTok U.S. App. See NSA Sec. 1.5.

<sup>59</sup> See NSA Secs. 8.4, 8.5.1.i.

<sup>60</sup> See NSA Secs. 8.4, 9.8, 9.10.

<sup>61</sup> See NSA Secs. 8.4, 8.5, 11.2.

interconnections between the Platform and the rest of the world and can block any such interactions that, in its discretion, are unexpected or unauthorized.<sup>62</sup> Oracle will also be responsible for assessing and reporting to the U.S. Government on an ongoing basis any risks posed to U.S. national security and User privacy identified in the course of its Source Code review.<sup>63</sup>

69. The NSA requires that all Protected Data provided or derived from use of the App, including data voluntarily provided by TikTok U.S. Users at registration and any heuristic or behavioral data gathered from use of the App, be transported from the App to the Platform in the Secure Oracle Cloud.<sup>64</sup> TTUSDS and Oracle will ensure that Protected Data is stored exclusively within the Secure Oracle Cloud and nowhere else, and Oracle will be charged with securing and monitoring all access to the stored Protected Data.<sup>65</sup> TTUSDS will control all requests for access, including requests pursuant to court orders or subpoenas. The NSA requires that no one outside the U.S. be allowed to view or have access of any Protected Data, including any employee of TTUSDS, Oracle, or a Dedicated Transparency Center located in a “Five Eyes” country, subject to limited exceptions under a set of “Limited Access Protocols.”<sup>66</sup>

70. The NSA requires that TTUSDS make a complete list of all vendors and third parties that provide services, code, or content related to the App or the Platform, and the TTUSDS Security Directors, with oversight from the Third-Party Monitor, must conduct a

---

<sup>62</sup> See NSA Secs. 8.5, 9.8, 9.17, 9.18.

<sup>63</sup> See NSA Sec. 9.18.

<sup>64</sup> See NSA Secs. 8.4, 11.5.

<sup>65</sup> See NSA Secs. 8.4, 9.8, 11.5.

<sup>66</sup> See NSA Secs. 11.8-11.9.

security review of each vendor, with disclosure of the list to the U.S. Government for review and approval.<sup>67</sup>

71. The NSA requires TTUSDS to establish a Content Advisory Council of external social media, free speech, and content moderation experts who are U.S. citizens.<sup>68</sup> TTUSDS and the Content Advisory Council will review a so-called “playbook” created by Petitioners that informs how the Recommendation Engine decides what content to recommend to particular users, both global users and TikTok U.S. Users. A copy of the “playbook” will also be given to the U.S. Government and Oracle. TTUSDS will have ultimate say on how the playbook and Recommendation Engine for the TikTok U.S. Platform make decisions for the App and will ensure that the Recommend Engine is trained exclusively within the Secure Oracle Cloud.<sup>69</sup> Oracle will test the Recommendation Engine to ensure it complies with the playbook, as reviewed and approved by TTUSDS and the Content Advisory Council.<sup>70</sup>

72. In addition to relying on TTUSDS, Oracle, and the Source Code Inspector to carry out NSA functions, the NSA contains heavy oversight monitoring and audit provisions, which will be carried out by yet three more independent U.S.-based entities that must be engaged by TTUSDS. These additional U.S. entities must be approved by and will have reporting and fiduciary responsibilities to the U.S. Government. They cannot have any prior involvement or contractual relationship with Petitioners.

---

<sup>67</sup> See NSA Secs. 13.1-13.5.

<sup>68</sup> See NSA Sec. 5.4.

<sup>69</sup> See NSA Sec. 9.13.

<sup>70</sup> See *id.*

73. The first of these is a Third-Party Monitor, which will be responsible for conducting ongoing oversight of the actual implementation of the NSA by TTUSDS, Oracle, and the Source Code Inspector.<sup>71</sup> The Third-Party Monitor will be a principal point of contact for the U.S. Government regarding compliance.<sup>72</sup> Second, the NSA requires a Third-Party Auditor to conduct an independent audit of compliance by Petitioners and TTUSDS upon request by the U.S. Government.<sup>73</sup> The U.S. Government must approve the audit plan. Finally, the NSA requires a Cybersecurity Auditor, which will conduct a more tailored technical audit of TTUSDS's and Oracle's compliance with implementation of the Source Code review processes, the establishment and operations of Dedicated Transparency Centers, the secure Build process, the deployment of the App, the deployment of the Platform in the Secure Oracle Cloud, and the storage and protection of Protected Data.<sup>74</sup>

74. In addition to this oversight, the U.S. Government retains the right to monitor all of Petitioners' and TTUSDS's compliance directly and to conduct inspections at its discretion. The U.S. Government can "inspect the books and records, equipment, servers, and facilities, and premises owned, leased, managed, or operated in the United States by [Petitioners as well as TTUSDS] for the purposes of monitoring compliance with or enforcing this Agreement; provided that in exigent circumstances, no advance notice is required. This right to access and inspect extends to the Personnel, books and records, equipment, servers, facilities, and premises of any third-party contractor or agent working on behalf of [Petitioners and any of their

---

<sup>71</sup> See NSA Secs. 16.1-16.6.

<sup>72</sup> See NSA Sec. 16.4.

<sup>73</sup> See NSA Sec. 15.1.

<sup>74</sup> See NSA Secs. 14.1-14.6.

Affiliates].”<sup>75</sup> The U.S. Government also retains access and inspection rights with respect to Oracle and its compliance with the NSA.<sup>76</sup>

75. The final critical element of the NSA is its collection of enforcement mechanisms. I have already mentioned one of them above—i.e., the ability of Oracle unilaterally to stop use of the App if ByteDance fails to fix security problems with the Source Code.<sup>77</sup> In addition to this provision related to Source Code review, the NSA contains a provision that authorizes the U.S. Government to shut down operations of the App and the Platform if (i) there are material violations of the NSA, (ii) Petitioners attempt to interfere with any aspect of the NSA, (iii) Oracle is denied access to the Dedicated Transparency Centers, (iv) there is any attempt by Petitioners to deploy any version of the App or Platform that has not been reviewed or deployed by Oracle, or (v) there is any actual or attempted unauthorized access to Protected Data.<sup>78</sup> In my experience with mitigation agreements, the magnitude of this unilateral enforcement authority given to the U.S. Government is unprecedented.

### *Caveats and Assumptions*

76. I now turn to analyzing the effectiveness of these terms of the NSA, in light of the risk model. However, before doing so, it is important to state certain caveats and assumptions.

77. I note that the only information I have relied upon in preparing this Declaration is the CFIUS record provided by Petitioners to the U.S. Government as well as widely accepted and publicly available facts. My opinion is based solely on those sources and not on anything

---

<sup>75</sup> See NSA Sec. 17.1.

<sup>76</sup> See NSA Sec. 17.2.

<sup>77</sup> See NSA Secs. 9.14-9.15.

<sup>78</sup> See NSA Secs. 21.3-21.5.

confidential or unavailable to the public. I have had no access to any classified information regarding this matter. Neither my description of the risk model nor my opinions herein are derived from or rely on classified or non-public information.

78. My first important assumption relates to the “threat” element of the risk model. I will assume for purposes of this Declaration that Petitioners are subject to at least influence if not control by Chinese interests. I understand that Petitioners disagree with this assumption, but analysis of this question is not within the scope of this Declaration. Based on this assumption, I will also assume without analyzing or opining that Congress and CFIUS considered Petitioners to pose HIGH threats.

79. In light of this assumption about Petitioners, I also assume without analyzing or opining that Congress and CFIUS would not be willing to trust Petitioners to faithfully comply with the NSA in the absence of some means of either ensuring trust or removing the requirement to trust Petitioners, such as the use of a trusted third party to be responsible for mitigation implementation.

80. My final assumption relates to the “consequences” posed by Petitioners control of or access to the App or the Platform. I will assume for purposes of this Declaration that if Protected Data is compromised or if the App or Platform is used to exploit content on the Platform, the national security consequences will be HIGH. Again, I am not analyzing this question and offer no opinion on the magnitude of the asserted consequences one way or the other. I understand Petitioners may disagree with this assessment, but the resolution of this question is not necessary to my analysis.

*Analysis of the NSA*

81. Because I am assuming a HIGH threat posed by Petitioners and a HIGH consequence to national security if vulnerabilities are exploited, my analysis is focused exclusively on the vulnerability analysis under the risk model. The seminal question is whether the NSA, if faithfully implemented as written, is sufficient to effectively mitigate vulnerabilities associated with Petitioners' control of the App and Platform, including access to Protected Data, such that the overall vulnerability assessment would be reduced to a LOW level.

82. As discussed above in connection with the risk model, the vulnerability analysis asks whether, by virtue of controlling a U.S. company or asset, a foreign "threat" actor would have sufficient access to allow it to capitalize and implement methods of exploitation to impair national security. In this case, the question is whether Petitioners could use their control, influence, or access to exploit the App or Platform to (i) use Protected Data to gather intelligence about U.S. persons, or (ii) use the Platform, including control of the Recommendation Engine, to engage in propaganda or misinformation campaigns either in China's favor or against the U.S.

83. As a threshold matter, I first consider whether the U.S. Government would be required to rely on Petitioners to faithfully comply with the NSA in order to mitigate national security risks. To reiterate, the U.S. Government has been reluctant to enter into mitigation agreements with companies based in China or under Chinese control because of concern that the Chinese government could force companies to subvert U.S. national security interests despite the existence of contractual mitigation requirements. The important exception to this reluctance has been where the U.S. Government has been able to rely on a trusted third party to ensure compliance such that blind reliance on a Chinese company is not required.

84. That is the case here. First, the NSA requires the creation of TTUSDS, which will have governance and operational independence. Its Board and management will be free from the control or influence of Petitioners. TTUSDS will be responsible for the core security functions (i.e., “CFIUS Functions”) that are at the heart of the NSA’s mitigation mechanisms.

85. Second, importantly, the NSA requires the use of a third-party TTP—Oracle—to be the technical overseer of the NSA and to deploy and operate the App and the Platform. Oracle is a trusted U.S. company, and under the terms of the NSA, Oracle will have responsibilities directly to the U.S. Government. Its economic incentives will align with U.S. Government interests because non-compliance could lead to the U.S. Government exerting its shut-down authority under the NSA, which would end what is certainly well-compensated work by Oracle under the master services agreement.

86. By using TTUSDS and Oracle, the U.S. Government is not required to rely on Petitioners’ compliance. It effectively means that U.S. citizens with obligations and loyalties to the U.S. Government will be in control of NSA implementation.

87. It is relevant to re-emphasize that this use of a secure U.S. subsidiary of a foreign parent is a well-recognized and long-used method for addressing national security risks. CFIUS has often used it, as has the FCC and “Team Telecom.” It is also used often by the Department of Defense to protect classified information and classified contracts from the control and influence of foreign parent companies.

88. The next step in the analysis is to look at whether Petitioners could still have sufficient access to exploit the App or the Platform, despite not having control or influence over TTUSDS or any of the mechanisms for deploying or operating the App or the Platform.



89. In the absence of Board or management control, a relevant question is whether Petitioners might still have the ability to manipulate or control the placement of co-opted employees in TTUSDS or Oracle or to influence decisions regarding vendors associated with the App or the Platform. The NSA effectively cuts off these vectors by imposing rules around TTUSDS hiring and controlling the ability of TTUSDS to use employees who are non-U.S. citizens or who have had a prior affiliation with Petitioners. These same hiring and vendor rules are imposed on Oracle.

90. Because the NSA cuts off these governance, management, and hiring/contracting vectors, the lone remaining potential access that could enable exploitation by Petitioners is through technical exploits of the App or the Platform. For purposes of clarity, it is important to re-emphasize that under the NSA, ByteDance will remain completely in control of developing Source Code for all of the components that comprise “TikTok”—the App and the Platform, including the Recommendation Engine. As stated above, I am assuming without concluding that this access could be used for exploiting vulnerabilities, such as misappropriating Protected Data or manipulating content on the TikTok Platform.

91. With that said, in my professional opinion, the NSA effectively cuts off this technical “access” vector and effectively mitigates the ability of Petitioners to exploit the App or the Platform. There are two technical access methods to consider. The first is whether by virtue of understanding the Source Code for the App and the Platform, Petitioners or some other third-party could gain control over and access to deployed Executable Code and configuration of the App and the Platform. The second is whether there may be self-executing functions, “backdoors,” or other exploits planted in the Source Code that could exploit the App or the

Platform even if Petitioners could not take control following deployment or control configuration.

92. On the first point—Petitioners using deployed Executable versions of the App and the Platform—as explained above, the NSA requires that all deployment and operations of the App and the Platform must emanate from and be controlled by TTUSDS within the Secure Oracle Cloud, including all application and network configurations. Oracle’s infrastructure will be the exclusive source in the U.S. for issuance of the App and the Platform. Petitioners will have no physical or logical access to the App or the Platform once signed Source Code and accompanying SBOMs are deposited in Dedicated Transparency Centers. All functionality and all interconnectedness for the Platform will be hosted on and run through the Secure Oracle Cloud. There may not be a more secure commercial cloud environment in the U.S. than the Secure Oracle Cloud. The NSA’s terms ensure that there will be no logical or physical access or interconnection points between the App and the Platform and any untrusted entity because TTUSDS, with Oracle serving as a trusted validator, will control the end-to-end process. Oracle will be able to view, inspect, and stop any traffic between the App and the Platform and well as all movement of Protected Data. Under the direction of TTUSDS, Oracle will have technical operational responsibility for the storage, protection, and control of Protected Data.

93. The second consideration relates to embedded self-executing exploits in the Source Code. As discussed at length above, a key component of the NSA is the Source Code review process. This falls under the responsibility of TTUSDS, Oracle, and an additional Source Code Inspector. It will be conducted within the Secure Oracle Cloud, after pulling Source Code and SBOMs from the Dedicated Transparency Centers. Oracle will enable the Source Code

Inspector to have full manual and automated access. No Source Code will enter the Build process until it is reviewed by Oracle.

94. Source Code review is a difficult and detailed process. However, highly trained reviewers are adept at understanding code. Automated tools for helping review code have greatly enhanced the effectiveness of Source Code review, including new tools empowered by artificial intelligence.

95. While it is hypothetically possible that some security flaws or even exploits could slip through the Source Code review process, it would be implausible as a practical matter for Petitioners to attempt to evade the NSA by embedding malicious code. First, there is a high likelihood of discovery. Both Oracle and the Source Code Inspector will be very highly trained in spotting malicious code, especially when using robust tools. The reviewers are experienced in spotting both intentionally malicious code as well as non-malicious vulnerabilities that emerge during the coding process.

96. Second, there will be immediate reporting to the Third-Party Monitor and the U.S. Government if malicious code is found.

97. Third, the use of SBOMs and signed code means that Oracle and the Source Code Inspector will be able to track the provenance of malicious code and identify quickly where it came from and when it arrived. Oracle and the Source Code Inspector will also be able to compare versions of Source Code that it reviewed and will be able to see when new features or commands have been added or removed, all of which will have to comport with SBOMs that accompany the reviewed Source Code.

98. All of this will enable not only reporting under the terms of the NSA, but if there is malicious intent or an attempt to compromise a protected computer or network, it could

become a federal criminal matter under the federal computer intrusion statute and, depending on the facts, could also be investigated or prosecuted as an attempt by a foreign power to take action against U.S. interests under national security statutes.

99. In addition, the NSA imposes rigorous broad oversight over the NSA's implementation, mandating the involvement of three additional independent monitors and auditors—the Third-Party Monitor, the Third-Party Auditor, and the Cybersecurity Auditor.

100. The provisions in the NSA that give the U.S. Government the ability to unilaterally stop the use of the App and the Platform for non-compliance is a high-water mark for U.S. Government control in a mitigation environment. The fact that there are six independent U.S. entities involved in NSA implementation and compliance—TTUSDS, Oracle, the Source Code Inspector, the Third-Party Monitor, the Third-Party Auditor, and the Cybersecurity Auditor—means that if any one of those entities catch or alert on non-compliance, it could trigger the process that could result in the U.S. Government putting a stop to the App and the Platform. It is a very broad net and would be a significant and complex set of obstacles to navigate even if there were an intent by Petitioners—or some other Chinese interest—to surreptitiously exploit vulnerabilities via the Source Code or the deployed App or Platform.

101. In addition to my experience and expertise with CFIUS and mitigation agreements, I am also a former counterespionage investigator and prosecutor. In my experience related to nation-state intelligence gathering efforts, when a potential avenue for intelligence collection is highly scrutinized and spotlighted, there are strong incentives to choose an alternate method and avoid detection. The App and the Platform are under intense scrutiny. The NSA will accelerate the scrutiny and visibility in an exponential manner. I believe Chinese interests,

even if they were otherwise motivated to want to exploit the App and the Platform, would choose alternate vectors of collection in order to avoid discovery.

102. My final point of analysis relates to the Recommendation Engine and the potential manipulation of content on the Platform to disseminate propaganda, squelch information that is harmful to Chinese interests, or foment disunity within the U.S. Access vectors for Petitioners to exploit this vulnerability, if they were to retain control of the Platform, would be to embed functionality in the Source Code for the Recommendation Engine or to manipulate the configuration of the Recommendation Engine, including feeding “training” data into it in an effort to sway how content is distributed. The NSA contains several provisions that would make misuse of the Recommendation Engine unlikely. First, the Source Code review likely will find security flaws. More importantly, the Recommendation Engine will be accompanied by a playbook that will be available to TTUSDS and Oracle, as well as to the Content Advisory Council, on how recommendations to users should look. The Third-Party Monitor will also be involved and will enable the U.S. Government to have a say in the playbook. Oracle, which will have complete and exclusive control of the deployed Recommendation Engine in the U.S., will be required to monitor its behavior against the playbook. Oracle will conduct testing and analysis to assess its behavior. In addition, all of the training (i.e., machine learning) for the Recommendation Engine will be done in the Secure Oracle Cloud using only training data in that Cloud, which means there will be no opportunity to train the Recommendation Engine on Chinese propaganda or misinformation. Only U.S. persons will be involved in the deployment and training of the Recommendation Engine.

103. Similar protections exist with respect to other processes for the promotion or filtering of TikTok content apart from the Recommendation Engine. The NSA requires

TTUSDS to ensure that only authorized personnel can engage in video promotion and filtering for the App and Platform and to document for the Third-Party Monitor how video promotion and filtering functions will be carried out. The Third-Party Monitor and the Third-Party Auditor can conduct audits to ensure promotion and filtering decisions are consistent with the playbook and other policies and are properly geared toward commercial purposes. Reports of those audits will be provided to the U.S. Government, which can conduct its own audits.

104. To be clear, I do not assess any one provision of the NSA as the single “silver bullet” that renders the NSA effective to mitigate national security risk. Rather, it is the combination of the level of independence granted to TTUSDS, reliance on multiple trusted third parties such as Oracle, the operational security processes, complex and thorough technical mitigations, as well as unprecedented oversight, monitoring, and very rigorous enforcement mechanisms, that lead me to conclude that the NSA effectively mitigates national security risk associated with the App and the Platform. Using the risk model described above, if the NSA were implemented as written, the overall vulnerability assessment associated with Petitioners owning and deploying the TikTok U.S. App and the TikTok U.S. Platform would be reduced to a LOW level. I cannot conceive of a more technically secure mitigation scheme for the App and the Platform in the U.S. than the scheme devised by the NSA.

## **CONCLUSIONS**

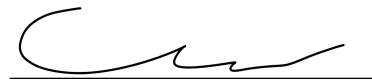
105. The risk model described above is the national security analytic model that is used by Congress, CFIUS, and other U.S. government entities to assess the effectiveness of the NSA to mitigate national security risk.

106. I have reviewed the NSA as well as the history of negotiations between CFIUS and Petitioners regarding the NSA.

107. Using the risk model, my professional opinion is that if implemented as written, the NSA would effectively mitigate the U.S. national security risks associated with Petitioners owning and deploying the TikTok U.S. App and the TikTok U.S. Platform.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this day June 17, 2024.

  
\_\_\_\_\_  
Christopher P. Simkins

**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/>		)	

**DECLARATION OF STEVEN WEBER**



I, Steven Weber, under penalty of perjury, hereby declare as follows:

1. I am a Professor of the Graduate School at the University of California, Berkeley (“UC Berkeley”), where I hold joint appointments as Professor at the School of Information and in the Department of Political Science. I am also the founder and former faculty director of the Center for Long Term Cybersecurity at UC Berkeley, where for seven years I led a multi-disciplinary research group that worked on emerging digital security issues at the confluence of new technologies, human behavior, and risk calculations made by firms and governments. In addition to my academic appointments, I am a Partner at Breakwater Strategy, a strategic insights and communications firm, where I assist clients with strategic decision-making and communications in areas that involve the intersection of technology and public policy. I received a Ph.D. in political science from Stanford University in 1989 and have been a professor at UC Berkeley since 1989.

2. My work focuses on U.S. national security issues with particular emphasis on how digital technologies impact and are impacted by national and international security. I have written three relevant university press peer-reviewed books and a number of peer-reviewed journal articles on this subject, as well as many other articles published in non-peer reviewed publications. I have served as a consultant to a wide variety of U.S. and global firms as well as U.S. government agencies dealing with strategic issues at the intersection of national security and the digital economy. A copy of my curriculum vitae is attached hereto as Appendix 1.

3. I have been retained by counsel for Petitioners TikTok Inc. and ByteDance Ltd. in this action to analyze certain reported justifications for the Protecting Americans from Foreign Adversary Controlled Applications Act (the “Act”), which was signed into law by President Biden on April 24, 2024. As I discuss below in greater detail, I understand that some have

suggested justifications for the Act focused on two issues: (1) the security of the data that TikTok collects from its U.S. users, particularly as it relates to alleged risks of disclosure to the Chinese government; and (2) the possibility that TikTok’s recommendation algorithm (*i.e.*, the computer code that selects what content to present in a user’s feed) could be misused for the benefit of the Chinese government, either by censoring certain content or promoting propaganda or disinformation.<sup>1</sup>

4. As I discuss below, these issues are not unique or even distinctive to TikTok. (By TikTok, I mean to refer to the platform as opposed to any particular corporate entity.) It is inherent in digital technologies that every company, governmental entity, or non-governmental organization faces risks to the security of the data that it creates, processes, transmits, and stores—whether on behalf of employees, customers, or others.<sup>2</sup> Major companies (including many with highly sophisticated security operations) such as Yahoo!, LinkedIn, Meta, Marriott, Experian, Adobe, UnitedHealth, and many others have suffered well-known data breaches of millions of user records.<sup>3</sup> And with respect to TikTok’s recommendation algorithm, I am unaware of any evidence that supports the contention that TikTok’s algorithm has been manipulated to promote propaganda or disinformation. Insofar as there is a concern that propaganda or disinformation *exists* on the platform, that is an issue that essentially all social

---

<sup>1</sup> Because the Act does not contain any legislative findings or a statement of purpose, I have reviewed statements from individual Members of Congress as well as other sources expressing possible justifications for the Act.

<sup>2</sup> See, e.g., *Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts*, U.S. Dep’t of Homeland Security (May 15, 2018), <https://perma.cc/EDJ4-Y3DP>.

<sup>3</sup> Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO Online (Nov. 8, 2022), <https://perma.cc/T3U4-8TPU>; see also Manas Mishra & Zeba Siddiqui, *UnitedHealth Says Hackers Possibly Stole Large Number of Americans’ Data*, Reuters (Apr. 22, 2024), <https://perma.cc/2DPZ-ZJUK>.

media and entertainment platforms are dealing with more generally—a fact the U.S. government has acknowledged in official intelligence reports.<sup>4</sup> YouTube, for example, has previously added disclaimers to certain channels that were reportedly being used to spread disinformation on behalf of the Russian government.<sup>5</sup> Meta issues quarterly reports on its efforts to respond to coordinated inauthentic behavior on its platforms and, in a recent report, announced that it had removed thousands of accounts originating in China and Russia that had engaged in coordinated inauthentic behavior in 2023.<sup>6</sup> Indeed, it is now common practice among major social media firms to work to identify and take down content and accounts that promote disinformation and to make regular public disclosures in which they offer details on these operations.<sup>7</sup>

5. In short, while there are legitimate policy issues regarding data security and the use of online platforms for propaganda and disinformation, they are industry-wide issues that are not unique to TikTok. Indeed, even if TikTok were able to implement the type of “qualified divestiture” contemplated by the Act, the concerns that animated the Act would remain, just as they do with respect to many other social media and entertainment platforms. To the extent that TikTok is different from its peers, moreover, it is distinguished by the commitments it has made to address the U.S. government’s stated concerns, which are expressed in the draft National

---

<sup>4</sup> Nat’l Intel. Council, Declassified Intelligence Community Assessment, *Foreign Threats to the 2020 U.S. Federal Elections* (Mar. 10, 2021), <https://perma.cc/JKF3-7KDC>.

<sup>5</sup> Paresh Dave & Christopher Bing, *Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels: Researchers*, Reuters (June 7, 2019), <https://perma.cc/SB9H-R76W>.

<sup>6</sup> Ben Nimmo, Nathaniel Gleicher, Margarita Franklin, Lindsay Hundley & Mike Torrey, *Third Quarter Adversarial Threat Report*, Meta (Nov. 2023), <https://perma.cc/R9HW-Y49Y>.

<sup>7</sup> See, e.g., *YouTube Community Guidelines Enforcement*, Google (last accessed June 12, 2024), <https://perma.cc/33PU-QN6S>; *Transparency Reports*, Meta (last accessed June 17, 2024), <https://perma.cc/AJE9-YWPL>; *Transparency Report*, July 1, 2023–December 31, 2023, Snap (last accessed June 12, 2024), <https://perma.cc/Q629-WU9K>; *Covert Influence Operations*, TikTok (last accessed June 12, 2024), <https://perma.cc/EF89-NNDH>.

Security Agreement and reflect protections for the integrity of TikTok data and content that go beyond industry norms.

6. With this introduction, I address in detail the two issues that have been cited by some Members of Congress as justifications for the Act: data security and the susceptibility of TikTok’s algorithm to foreign government influence.

**I. Data Security**

7. The first justification that some have suggested for the Act is a perceived need to protect U.S. TikTok users’ “data security.”<sup>8</sup> According to a House Committee Report for an earlier version of the Act, mobile applications, including those purportedly controlled by foreign adversaries, can “collect vast amounts of data on Americans.”<sup>9</sup> The House Committee Report expressed a concern that data collected through mobile applications could be used by a foreign adversary to “conduct espionage campaigns,” including by tracking specific individuals.<sup>10</sup>

8. As an initial matter, the assertion that mobile applications, including TikTok, “collect vast amounts of data on Americans” is principally a statement about data privacy, not data security. There is a separate policy debate about the extent to which social media and other digital product companies collect information from users, and this debate is beyond the scope of my testimony. I note, however, that the type and amount of data that TikTok collects from U.S. users—which is disclosed to users pursuant to TikTok’s Privacy Policy, to which users agree as a

---

<sup>8</sup> Jane Coaston, *What the TikTok Bill Is Really About, According to a Leading Republican*, N.Y. Times (Apr. 1, 2024), <https://perma.cc/B2YN-7QFK> (quoting the Act’s original sponsor, Representative Mike Gallagher).

<sup>9</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>10</sup> *Id.* at 2, 4.

condition of signing up for the app—is comparable to the type and amount of data that other social media platforms and applications collect from U.S. users.<sup>11</sup> In other words, the data collected by TikTok is not meaningfully different—either in amount or kind—from the data that other applications collect, including applications owned by U.S. companies like Google, Snap, and Meta.<sup>12</sup>

9. Social media and online entertainment platforms are also not unique in collecting data from users. A wide variety of mobile applications collect significant amounts of user data, such as weather apps that collect precise geolocation data and device information.<sup>13</sup> Indeed, some apps have been shown to collect categories of information that bear little or no relationship to the business purpose of the app at all—such as utility apps (like a flashlight app on a cell phone) that collect geolocation and other non-pertinent data.<sup>14</sup>

---

<sup>11</sup> Milton L. Mueller & Karim Farhat, *TikTok and U.S. National Security*, Georgia Inst. of Tech. Internet Governance Project, at 19 (2023), <https://perma.cc/JR3Z-F5TK> (explaining that “TikTok’s behavior is not suspicious and it is not exfiltrating unusual data” and that “[w]hile TikTok collect[s] many data items, overall they still fall within general industry norms for user data collection” (citation omitted)).

<sup>12</sup> It is worth noting that, in some respects, TikTok collects more limited data than other mobile applications. For example, the current version of the TikTok app does not collect precise or approximate GPS data from U.S. users. See *Mythbusting: The Facts on Reports about Our Data Collection Practices*, TikTok (Feb. 22, 2023), <https://perma.cc/GS8A-W9FC>. Additional transparency around the data TikTok collects is now also available by virtue of TikTok storing such data in the Oracle Corporation cloud environment, as discussed below.

<sup>13</sup> Thorin Klosowski, *We Checked 250 iPhone Apps—This Is How They’re Tracking You*, N.Y. Times (May 6, 2021), <https://perma.cc/9YS5-AECB>; Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), <https://perma.cc/B5AU-YLKP>.

<sup>14</sup> *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, Fed. Trade Comm’n (Dec. 5, 2023), <https://perma.cc/KN96-7TTL>.

10. Although the assertion that TikTok “collect[s] vast amounts of data on Americans” is primarily a statement about data privacy, the assertion that user data collected by TikTok could be used by a foreign adversary to “conduct espionage campaigns” is an assertion about data security because it is a statement regarding who has access to data and for what purpose. The validity of this statement can therefore be analyzed based on principles of data security.

11. Before proceeding with the analysis, there are two general information security principles that should be kept in mind. First, data security is not a binary switch that can be toggled on or off. There are always tradeoffs being made among three components of security: confidentiality, integrity, and availability of data.<sup>15</sup> As with many enterprise risks, data security is an exercise in risk management—identifying risks, assessing them, and mitigating those risks to acceptable levels.<sup>16</sup>

12. Second, when it comes to data security threats, it is virtually impossible to prove the negative and establish that there are *no* risks associated with a particular application, network, or data storage and management system.<sup>17</sup> Sophisticated organizations and information security professionals base their work on the foundational proposition that malicious actors and technology are constantly evolving, which means the threat landscape is always changing. Even

---

<sup>15</sup> This three-part framework is explained by the National Institute of Standards and Technology in *Standards for Security Categorization of Federal Information and Information Systems*, Fed. Info. Processing Standards Publication 199 (Feb. 2004), <https://perma.cc/52R4-XE3H>.

<sup>16</sup> *Cybersecurity Strategy*, U.S. Dep’t of Homeland Security (May 15, 2018), <https://perma.cc/5UUV-ZVE7>; Nat’l Inst. of Standards & Tech., *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 Rev. 5, at 13 (Sept. 2020), <https://perma.cc/KY6M-4TF9>.

<sup>17</sup> Shuman Ghosemajumder, *You Can’t Secure 100% of Your Data 100% of the Time*, Harv. Bus. Rev. (Dec. 4, 2017), <https://perma.cc/22XX-DQLU>.

an organization with state-of-the-art security practices across the board cannot, with full confidence, assert that there is no risk that its data could be vulnerable to attack or inadvertently accessed, improperly accessed, or disclosed. These principles form the basis of sophisticated data security programs and strategies in advanced organizations.

13. With these general principles in mind, turning to the specific asserted national security concerns related to TikTok’s user data, it is important to first assess the type of data we are discussing. As a recent report by the Internet Governance Project at the Georgia Institute of Technology (“Georgia Tech”) explained, “[f]ull access to all TikTok data would provide [an actor with] aggregate data about the user population’s video uploading and consumption behavior.”<sup>18</sup> As the report explained, while such information may be “commercially valuable” to TikTok as well as certain developers and advertisers, it is unlikely to be particularly valuable to a foreign state like China, as it provides no “special insight into the control of critical infrastructure, military secrets, opportunities for corporate espionage, or knowledge of weapons systems.”<sup>19</sup>

14. Even assuming some national security-related intelligence value for high-value targets (*e.g.*, individuals of particular interest from an intelligence perspective) could be derived from collecting a data set of commercially-focused information, the notion that the Chinese government would seek to amass this intelligence information by appropriating TikTok user data is not plausible, given the alternative means available to a nation state interested in acquiring information about individuals in another country. Those alternatives include conducting open source intelligence gathering from public information sources (including LinkedIn, Facebook,

---

<sup>18</sup> Mueller & Farhat, *supra* n.11, at 20.

<sup>19</sup> *Id.*

and other platforms) where people regularly disclose information about themselves that could be valuable to an intelligence program; and direct cyberattack operations like China's reported intrusion into the database of the U.S. Office of Personnel Management ("OPM") as well as Russia's reported theft of certain email correspondence between U.S. government agencies and Microsoft through a breach of Microsoft's software systems.<sup>20</sup>

15. Another avenue by which a nation-state actor may acquire information about high-value targets is by purchasing such information on the open market. Historically, there has been little regulation of the U.S. data brokerage industry, which is comprised of thousands of companies that collect, sell, and distribute individuals' data. At the same time as it passed the Act, Congress also passed legislation that places certain restrictions on data brokers' ability to transfer certain categories of information to "foreign adversary countr[ies]" (defined to include China, Russia, Iran, and North Korea) as well as entities "controlled" by such foreign adversary countries.<sup>21</sup> The legislation, however, does not forestall a foreign adversary's ability to purchase U.S. user data through the broader, multilayered data brokerage market. The recently passed legislation, for example, applies only to "data broker[s]," a statutorily defined term with enumerated exceptions.<sup>22</sup> Commentators have also noted that the legislation does not regulate

---

<sup>20</sup> Josh Fruhlinger, Ax Sharma & John Breeden, *15 Top Open-Source Intelligence Tools*, CSO Online (Aug. 15, 2023), <https://perma.cc/7TFG-KSCH>; Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO Online (Feb. 12, 2020), <https://perma.cc/L9SV-N6SY>; Sean Lyngaas, *Russian Hackers Steal U.S. Government Emails with Microsoft, Officials Confirm*, CNN (Apr. 11, 2024), <https://perma.cc/P7DF-96EV>.

<sup>21</sup> H.R. 815, div. I, § 2(a), 118th Cong., Pub. L. No. 118-50 (Apr. 24, 2024).

<sup>22</sup> *Id.* § 3. For example, the legislation defines a "data broker" to include entities that "sell[], license[], rent[], trade[], transfer[], release[], disclose[], provide[] access to, or otherwise make[] available data of United States individuals, that the entity did not collect directly from such individuals." *Id.* Entities that sell the "data of United States individuals" that they themselves "collect directly from such individuals" fall outside the definition.



the sale of U.S. user data to intermediary entities who may, in turn, sell or provide the purchased data to foreign adversaries.<sup>23</sup> Given these and other limitations, there are still a variety of ways by which a nation-state actor, like China, can obtain U.S. user data from the data broker ecosystem, notwithstanding the recent enactment of legislation designed to regulate brokers.

16. Given the existence of more effective and efficient means of obtaining relevant information about high-value targets, it is unlikely that China would seek to compel TikTok to turn over user data for intelligence-gathering purposes. Data security professionals generally work from the proposition that attackers will choose the path of least resistance to achieve their objectives. A review of cybersecurity breaches over the last decade bears this assumption out: the vast majority of attacks are not the most technically sophisticated operations (that often receive the most attention among specialists), but are instead much simpler attacks carried out through mundane vulnerabilities, such as unchanged default passwords and the lack of two-factor authentication.

17. Another reported reason for the Act is TikTok's asserted ties to China, which Members of Congress have suggested increase the vulnerability of U.S. TikTok data to misappropriation. A House Committee Report for an earlier version of the Act asserts that because affiliates of TikTok Inc.'s parent company, ByteDance Ltd., are headquartered in China and employ Chinese citizens, TikTok user data is less secure than data collected and maintained by other apps and platforms.<sup>24</sup> According to the report, under Chinese law, "the [Chinese

---

<sup>23</sup> Justin Sherman, *The Pros and Cons of the House's Data Broker Bill*, Lawfare (Apr. 11, 2024), <https://perma.cc/5BTM-FW9N>.

<sup>24</sup> House Committee Report at 3–4. TikTok has pointed out that ByteDance Ltd. is a Cayman Islands holding company, and that its operating entities in China are subsidiaries of ByteDance Ltd. References in this declaration to "ByteDance" are to the corporate group, rather than any particular entity.

government] can require a company headquartered in [China] to surrender all its data to the [Chinese government], making companies headquartered [in China] an espionage tool of the CCP [Chinese Communist Party].”<sup>25</sup> The report further contends that TikTok “rel[ies] on . . . engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application,” “potentially expos[ing] U.S. users to malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development.”<sup>26</sup> Finally, the report contends that ByteDance “has close ties to the CCP, including a cooperation agreement with a security agency and over 130 CCP members in management positions.”<sup>27</sup>

18. From a data security perspective, these asserted ties to China do not distinguish TikTok from other multinational corporations that create, maintain, and utilize U.S. user data. With respect to the concern that the Chinese government may require ByteDance to surrender data on U.S. TikTok users, it bears emphasis that many U.S. technology companies—including Cisco, Dell, Electronic Arts, Hewlett-Packard, IBM, LiveRamp, and Palo Alto Networks—have Chinese-headquartered subsidiaries, and therefore face the same theoretical risk that Chinese government officials may seek to compel disclosure of customer or user data from those companies.<sup>28</sup> Moreover, a number of apps and platforms that appear to have connections to and

---

<sup>25</sup> *Id.* at 4; see also *Threat Posed by TikTok*, U.S. Dep’t of Justice (Mar. 6, 2024) (“[The Chinese government’s] national security law requires any company doing business in China to make its data accessible to the [Chinese] government and to support its intelligence efforts.”).

<sup>26</sup> House Committee Report at 5.

<sup>27</sup> *Id.* at 7.

<sup>28</sup> Cisco Systems, Inc., Annual Report (Form 10-K) (Sept. 7, 2023); Dell Technologies Inc., Annual Report (Form 10-K) (Mar. 25, 2024); Electronic Arts Inc., Annual Report (Form 10-K) (May 22, 2024); HP Inc., Annual Report (Form 10-K) (Dec. 15, 2023); International Business Machines Corporation, Annual Report (Form 10-K) (Feb. 26, 2024); LiveRamp Holdings, Inc.,

operations in China—such as Temu and Shein, two popular e-commerce apps in the United States—collect and maintain U.S. user data as well.<sup>29</sup>

19. With respect to the concern that ByteDance relies on “engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application,” many U.S. companies maintain software and other engineering operations in China. Electronic Arts, for example, maintains a major development studio in China that, as of June 2024, has over 400 employees.<sup>30</sup> These employees, many of whom are Chinese citizens, work on developing popular video games, such as FIFA and The Sims,<sup>31</sup> both of which have millions of U.S. and international users.<sup>32</sup> Such companies’ Chinese operations reflect that the issues identified in the House Committee Report are, once again, not unique to TikTok, but instead are industry-wide issues. Indeed, companies face risks that “engineers and back-end support” may engage in “problematic activities tied to source code development,” regardless of whether those companies have offices or operations in China. For example, earlier this year, a former Google software engineer based in California was indicted on charges of stealing trade secrets related to

---

Annual Report (Form 10-K) (May 22, 2024); Palo Alto Networks, Inc., Annual Report (Form 10-K) (Sept. 1, 2023).

<sup>29</sup> Nicholas Kaufman, *Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes*, U.S.-China Econ. & Security Review Comm’n (Apr. 14, 2023), <https://perma.cc/8X32-DSDR>; Mark A. Green, *It Isn’t Just TikTok: Americans Like Other Chinese-Owned Apps Too*, Wilson Ctr. (May 2, 2023), <https://perma.cc/Z5FT-MV7G>.

<sup>30</sup> *EA China*, Electronic Arts (last accessed Jun. 12, 2024), <https://perma.cc/Y43K-GKKV>.

<sup>31</sup> *Id.*

<sup>32</sup> *The Sims 4 Becomes the Most Widely Played Game in the 23 Year History of the Franchise With More Than 70 Million Players Worldwide*, Electronic Arts (Apr. 18, 2023), <https://perma.cc/57E4-K2JD>; *FIFA 23*, Active Player (last accessed Jun. 12, 2024), <https://perma.cc/8937-UEZ5>.

artificial intelligence systems in development at Alphabet, allegedly to benefit two Chinese companies the engineer was secretly working for.<sup>33</sup>

20. Finally, the fact that ByteDance reportedly employs certain CCP members is likewise not a distinguishing feature of TikTok. As U.S. government officials have acknowledged, virtually all major Chinese companies are required to maintain internal committees comprised of CCP members, and in recent years, a number of U.S. companies doing business in China have instituted such committees of their own.<sup>34</sup> There is evidence that many of these CCP committees are purely symbolic in nature.<sup>35</sup> But even if they are not, the assertion that ByteDance maintains an internal CCP committee does not distinguish the company from other companies with CCP committees (including both Chinese and U.S. companies) that are not treated the same way as TikTok under the Act.

21. There is one material respect, however, in which it is possible to distinguish TikTok from other industry participants when it comes to the data security concerns that were

---

<sup>33</sup> Karen Freifeld & Jonathan Stempel, *Former Google Engineer Indicted for Stealing AI Secrets to Aid Chinese Companies*, Reuters (Mar. 6, 2024), <https://perma.cc/F4PZ-JHW3>.

<sup>34</sup> Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, Hudson Inst. (July 7, 2020), <https://perma.cc/4JNC-N3AY>; John K. Costello, Mem. for the Secretary, Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942 (Sept. 17, 2020), at 7 (noting that, as of 2017, CCP committees “existed in around 70 percent of 1.86 million private owned companies in China”).

<sup>35</sup> Joris Mueller, Jaya Wen & Cheryl Wu, *The Party and the Firm*, Working Paper (Dec. 2023), at 2, 5–6, <https://perma.cc/P3YV-V88S> (explaining that “[p]arty influence is more rhetorical than behavioral among domestic private and foreign-owned firms”); Lauren Yu-Hsin Lin & Curtis Milhaupt, *Party Building or Noisy Signaling? The Contours of Political Conformity in Chinese Corporate Governance*, 50 J. Legal Stud. 187, 189–90 (2021) (explaining that privately owned enterprises in China that have adopted charters providing for internal CCP committees “have largely limited their adoptions to symbolic provisions” and have not “acced[ed] to institutionalized party involvement in corporate governance”).

raised by Members of Congress, and that is the company's efforts to address the U.S. government's concerns through a national security agreement. I have reviewed the draft National Security Agreement ("NSA") that TikTok Inc. negotiated with the Committee on Foreign Investment in the United States ("CFIUS"), which I understand was designed to alleviate certain national security concerns identified by CFIUS concerning the U.S. TikTok platform. I am not an expert on the CFIUS process in particular, and I am not offering an opinion on the CFIUS review in this case. In my view, however, the relevance of the draft NSA is not limited to the specific confines of the CFIUS process. Rather, the draft NSA can be assessed more broadly as a set of commitments intended to mitigate a set of perceived national security risks, and the effectiveness of the draft NSA can also be analyzed on those terms, without regard to the specific parameters of the CFIUS review process.

22. Analyzing the draft NSA on those terms, it is my opinion that it provides for a robust system of controls to mitigate data security risks that might arise were foreign governments or adversarial groups acting as their agents to attempt to access protected U.S. user data. Moreover, in my view, these proposals significantly exceed and improve upon the controls that have been proposed and reportedly implemented by other social media and technology companies, including U.S. companies.

23. Pursuant to the NSA, TikTok Inc. has agreed to form a special-purpose subsidiary, TikTok U.S. Data Security Inc. ("USDS"), to oversee security-related issues.<sup>36</sup> USDS would be overseen by a special board of Security Directors, whose appointment would be subject to the U.S. government's approval.<sup>37</sup> The NSA further provides that protected U.S. user

---

<sup>36</sup> NSA arts. 2, 3, 8 & 11.

<sup>37</sup> *Id.* § 3.1.

data would be stored in the cloud environment of a U.S.-government-approved partner, Oracle Corporation (“Oracle”), with access to such data managed exclusively by USDS.<sup>38</sup> The NSA also provides for an extensive, independent third-party cybersecurity audit with multiple layers of review.<sup>39</sup> The NSA also includes a “shut-down option” that would allow the U.S. government to suspend TikTok in the United States if TikTok Inc. does not abide by certain obligations under the agreement.<sup>40</sup>

24. I understand that TikTok Inc. has started voluntarily implementing certain provisions of the NSA, including by incorporating and staffing USDS and partnering with Oracle on the migration of the U.S. TikTok platform and protected U.S. user data to the Oracle cloud environment.<sup>41</sup> I am not aware of any other online platform or service that maintains organizational and functional data security controls of the kind that have been proposed under the NSA.<sup>42</sup>

---

<sup>38</sup> *Id.* arts. 8 & 9.

<sup>39</sup> *Id.* § 14.1.

<sup>40</sup> *Id.* §§ 21.3–5.

<sup>41</sup> *About Project Texas*, TikTok (last accessed June 12, 2024), <https://perma.cc/W8Q5-F5Y6>.

<sup>42</sup> Zoom Video Communications (“Zoom”), for example, has adopted some—but not all—of the protocols contemplated by the draft NSA. Zoom has created a separate product—Zoom for Government—that includes security features beyond those included in Zoom’s standard product and processes communications “exclusively in continental U.S. data centers that are managed solely by U.S.-based, U.S. people.” Josh Rogin, *The White House Use of Zoom for Meetings Raises China-Related Security Concerns*, Wash. Post (Mar. 3, 2021), <https://perma.cc/M5GV-NS6Z>. TikTok, by contrast, is restructuring the company to maintain a version of the TikTok platform for the United States in a U.S. subsidiary; erecting software barriers to isolate the U.S. version of the TikTok app within the Oracle cloud; and granting Oracle—a U.S. company—access to its underlying source code.

25. Members of Congress have expressed particular concerns about the ability of the Chinese government to use TikTok to track specific individuals, including journalists.<sup>43</sup> This concern appears to be based on press reports that a few ByteDance employees used their previous access to certain TikTok user data to attempt to determine whether certain U.S.-based journalists were meeting with TikTok personnel who were suspected of leaking confidential information.<sup>44</sup> As with the other data security issues discussed above, the data security concerns raised by this episode relate to an industry-wide issue: the potential access to, and misuse of, data by corporate insiders for purposes not authorized by company policy. For example, Google has reportedly terminated dozens of employees between 2018 and 2020 for abusing their access to the company's tools or data, including with respect to accessing Google user data.<sup>45</sup> As another example, in November 2022, Meta reportedly fired or disciplined more than two dozen employees and contractors who inappropriately took control of Facebook user accounts.<sup>46</sup> And Uber has settled claims related to the company's "God View" tool, which reportedly allowed employees to track the location of Uber riders without obtaining their permission.<sup>47</sup> Indeed, even

---

<sup>43</sup> House Committee Report at 4, 8.

<sup>44</sup> Emily Baker-White, *Lawmakers Express Outrage that TikTok Spied on Journalists*, Forbes (Dec. 23, 2022), <https://perma.cc/G8ZF-ERR6>; Emily Baker-White, *TikTok Spied on Forbes Journalists*, Forbes (Dec. 22, 2022), <https://perma.cc/45YP-QVPK>; Mitchell Clark & Alex Heath, *TikTok's Parent Company Accessed the Data of US Journalists*, The Verge (Dec. 22, 2022), <https://perma.cc/N4EJ-DHXX>.

<sup>45</sup> Joseph Cox, *Leaked Document Says Google Fired Dozens of Employees for Data Misuse*, Vice (Aug. 4, 2021), <https://perma.cc/96LZ-39DH>.

<sup>46</sup> Rohan Goswami, *Meta Reportedly Disciplined or Fired More than Two Dozen Workers for Taking Over Facebook User Accounts*, CNBC (Nov. 17, 2022), <https://perma.cc/GY4Q-6D72>.

<sup>47</sup> Chris Welch, *Uber Will Pay \$20,000 Fine in Settlement Over 'God View' Tracking*, The Verge (Jan. 6, 2016), <https://perma.cc/43QZ-42UK>; Brian Fung, *Uber Settles with FTC Over 'God View' and Some Other Privacy Issues*, L.A. Times (Aug. 15, 2017), <https://perma.cc/U82U-4B44>.

outside the technology industry, the potential misuse of customer data by corporate insiders is a compliance challenge for virtually all companies.<sup>48</sup>

26. In the case of TikTok, it has been reported that the company investigated the misconduct, disclosed its findings, took action against the employees involved, and implemented remediation efforts, including a restructuring of the department in which the employees involved in the misconduct were employed and reforms meant to strengthen the company's internal controls.<sup>49</sup> This is consistent with how other companies have handled incidents of this kind.<sup>50</sup> From a data security perspective, TikTok's actions reflect an industry-best-practice response to an economy-wide compliance challenge, not a unique and extraordinary national security threat that would support consideration of an outright ban or divestment of the platform involved.<sup>51</sup>

## II. Susceptibility of TikTok's Algorithmic Recommendation System to Outside Influence

27. The second justification that some have suggested for the Act pertains to TikTok's algorithmic recommendation system, which certain Members of Congress have

---

<sup>48</sup> *Credit Suisse Staffer Took Salary Data*, Reuters (Feb. 13, 2023), <https://perma.cc/DHR2-7NYQ> (reporting that former Credit Suisse staffer misappropriated employee salary data as well as bank account information, Social Security numbers, and addresses); *Supermarket Morrisons Sued by Staff Over Personal Data Leak*, BBC News (Oct. 9, 2017), <https://perma.cc/CJQ9-M6CG> (reporting that former grocery store employee misappropriated employees' personal data).

<sup>49</sup> David Shepardson, *ByteDance Finds Employees Obtained TikTok User Data of Two Journalists*, Reuters (Dec. 22, 2022), <https://perma.cc/499P-JWHE>.

<sup>50</sup> Cox, *supra* n.45; Goswami, *supra* n.46.

<sup>51</sup> The arbitrariness of the Act's approach to data security is underscored by the Act's exemption for companies that operate a website or application "whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." *See* Act § 2(g)(2)(B). Websites or applications that "allow users to post product reviews, business reviews, or travel information and reviews" also frequently collect data from users. I am unaware of any national security-based reason for exempting companies that maintain such websites and applications from coverage under the Act.



suggested could be used to disseminate propaganda or otherwise mislead the American public.<sup>52</sup> For example, Representative Mike Gallagher, one of the Act’s co-sponsors, stated that TikTok presents a “propaganda threat” to the United States by “placing the control of . . . information—like what information America’s youth gets—in the hands of America’s foremost adversary [*i.e.*, China].”<sup>53</sup> Representative Raja Krishnamoorthi, another of the Act’s co-sponsors, stated that “the [TikTok] platform continue[s] to show dramatic differences in content relative to other social media platforms.”<sup>54</sup> And Representative Chip Roy, a member of the House Select Committee on the CCP, stated that “[TikTok] is . . . poisoning the minds of our youth every day on a massive scale.”<sup>55</sup> These statements could be construed to suggest that foreign actors, including China, may be using TikTok to influence users’ allegiances or belief systems by promoting and/or censoring certain content; alternatively, they could be interpreted as criticisms of the content available on TikTok irrespective of any such alleged manipulation. For purposes of this declaration, I focus on the allegation that TikTok is being used to manipulate users’ belief systems in furtherance of the aims of a foreign actor.

28. Before assessing these specific allegations, it is important to be clear about the applicable terminology. Specifically, it is important to draw a threshold distinction between “censorship” and “content moderation.” The two concepts are not the same. The issue around

---

<sup>52</sup> House Committee Report at 2, 7–8.

<sup>53</sup> Coaston, *supra* n.8 (quoting Representative Gallagher).

<sup>54</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/3C6F-7P4V>.

<sup>55</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/Q7DH-853D>.

ensorship here is whether an algorithm is being used to downgrade, remove, or prevent the creation of content that expresses opinions that the censor finds objectionable for illegitimate reasons. Content moderation, by contrast, refers to the legitimate removal or restriction of content that violates platforms' stated policies and the law. Here again, the practice of content moderation is an industry-wide issue and not an issue or practice limited to TikTok. X (formerly known as Twitter) attempts to block violence-promoting tweets.<sup>56</sup> Meta has an evolving set of policies that attempt to block various kinds of hate speech.<sup>57</sup> YouTube has modified its content moderation policies in an attempt to reduce radicalization, and in fact, the company reports that it removed over 9 million videos from the site in the 3-month period spanning October to December 2023.<sup>58</sup>

29. It is similarly important to draw a distinction between “propaganda” and “content recommendation” or “content promotion.” Much like the discussion of censorship, the issue of propaganda here is whether an algorithm is being used to promote or distribute content in order to influence or manipulate an audience for some illegitimate purpose. Content recommendation or promotion, by contrast, refers to the recommendation and/or promotion of certain content to users for legitimate business purposes. Here again, the practice of content recommendation and promotion is an industry-wide phenomenon. For example, for many years, YouTube partnered with creators to create original content for the site, which the company distributed through its

---

<sup>56</sup> *The X Rules*, X (last accessed June 12, 2024), <https://perma.cc/RJL9-62CS>.

<sup>57</sup> *Community Standards*, Facebook (last accessed June 12, 2024), <https://perma.cc/5CMJ-UWCK>.

<sup>58</sup> *YouTube Community Guidelines Enforcement* (last accessed June 12, 2024), YouTube, <https://perma.cc/8P6N-W6Q5>.

YouTube Originals page.<sup>59</sup> Instagram uses a variety of artificial intelligence tools to select, rank, and deliver content to a user’s “Explore” page, which has a clear business purpose, to facilitate users’ access to content they might like.<sup>60</sup>

30. From a national security perspective, the question is whether the algorithm is legitimately shaping the flow of content in accordance with a commercial product strategy, along with appropriate restrictions to counter proscribed activity (such as hate speech) consistent with its public Terms of Service; or whether the algorithm is illegitimately seeking to manipulate perspectives and opinions in directions that serve a foreign state’s short- and long-term strategic interests, which may be at odds with those of the United States.

31. Specifically with regard to TikTok, the question can be stated as follows: Is there evidence and reason to believe that TikTok is now or would become essentially an algorithmic propaganda tool of the Chinese government or the Chinese Communist Party? Based on the information that I have reviewed, my answer to this question is “no.”

32. As an initial matter, a small number of anecdotes about allegedly “censored” or “promoted” content do not in and of themselves demonstrate either the use of a platform for propaganda purposes or, even more so, a national security risk. That is partly because algorithmic content moderation and user experience customization are based on a fast-evolving science that involves state-of-the-art machine learning techniques to solve some of the hardest problems in content recognition, natural language processing, and other technology that sometimes go under the label of “artificial intelligence.” Like humans, algorithms can make

---

<sup>59</sup> Todd Spangler, *YouTube Shuts Down Original Content Group*, Variety (Jan. 18, 2022), <https://perma.cc/B7AD-CADB>.

<sup>60</sup> *How Posts Are Chosen for Explore on Instagram*, Instagram (last accessed June 12, 2024), <https://perma.cc/M9LG-YVEE>.

mistakes and then learn from those mistakes. In most companies, algorithmic moderation is supplemented by human content moderators who typically make assessments about “gray” or uncertain cases where algorithmic decision-making is ambiguous or inconsistent, as well as overseeing how algorithms perform relative to the platforms’ policies. The question, accordingly, is whether and how social media platforms react and evolve as they develop their technologies and practices over time and in response to ambiguous cases, concerns, complaints, and errors.

33. TikTok Inc.’s commitments in the draft NSA indicate that it is willing to respond to concerns about content moderation. For example, the NSA provides that all content moderation on the TikTok U.S. platform—both human and algorithmic—would be subject to third-party verification and monitoring.<sup>61</sup> Moreover, the NSA provides that the TikTok U.S. platform and application would be deployed through the Oracle cloud infrastructure, and Oracle and another third-party partner (to be approved by the U.S. government) would have access to TikTok’s source code.<sup>62</sup> Oracle and the third-party partner would review and vet TikTok’s source code and conduct inspections and tests of TikTok’s recommendation algorithm to ensure that it is acting in conformance with TikTok’s publicly stated, published content policies.<sup>63</sup> Oracle would report the findings of its inspections to the Security Directors (discussed above), after which the NSA contemplates that TikTok and Oracle would work to implement any necessary changes to TikTok’s software based on Oracle’s findings.<sup>64</sup>

---

<sup>61</sup> NSA §§ 5.4, 9.13, 16.6.

<sup>62</sup> *Id.* §§ 8.4, 9.1, 9.11.

<sup>63</sup> *Id.* § 9.13.

<sup>64</sup> *Id.*

34. Once again, I am unaware of any other major social media or entertainment platform that has committed to the level of transparency and extensive controls proposed under the NSA.

35. Recent academic studies further indicate that TikTok is honoring its commitment to responsible and viewpoint-neutral content moderation practices, notwithstanding certain anecdotal press reports to the contrary. For example, a 2023 report from Georgia Tech’s Internet Governance Project (referenced above) found that videos depicting “content . . . known to be major Communist Party taboos,” including “[s]upport for Hong Kong democracy protesters,” were “easily . . . found on TikTok,”<sup>65</sup> rebutting earlier press reports that such videos were uncommon on TikTok.<sup>66</sup> The report also found that searches related to the Chinese government’s treatment of the Uyghur minority, an ethnic minority group based in China’s Xinjiang Province, produced a list of search terms and videos “that by themselves are likely illegal on Chinese social media.”<sup>67</sup> Such evidence indicates that TikTok is neither promoting pro-China content nor censoring content that may be critical of China in a systematic way that supports allegations of a propaganda or disinformation campaign.

36. Certain Members of Congress—including Senator Mitt Romney and Representative Mike Lawler—have suggested that passage of the Act was motivated, at least in part, by concerns that TikTok has promoted pro-Palestinian content in the aftermath of Hamas’s

---

<sup>65</sup> Mueller & Farhat, *supra* n.11, at 12–13.

<sup>66</sup> Drew Harwell & Tony Romm, *Inside TikTok: A Culture Clash Where U.S. Views about Censorship Often Were Overridden by the Chinese Bosses*, Wash. Post (Nov. 5. 2019), <https://perma.cc/HX57-WYRK>.

<sup>67</sup> Mueller & Farhat, *supra* n.11, at 13.

October 7, 2023 attacks on Israel and the ongoing conflict in Gaza.<sup>68</sup> This assertion, however, rests on faulty inferences drawn from data—including the number of videos on TikTok with purportedly pro-Palestinian hashtags as compared to videos with pro-Israeli hashtags—that has been taken out of context. For example, it has been reported that, as of late October 2023, videos posted with the hashtag “standwithpalestine” had 10 times as many views on TikTok as videos posted with the hashtag “standwithisrael.”<sup>69</sup> But subsequent reporting has clarified that this 10-to-1 statistic includes view counts from TikTok users located outside of the United States as well as view counts dating back to 2020, well before the October 7 attacks.<sup>70</sup> This is significant because reporting has shown that videos with pro-Palestinian hashtags are overwhelmingly created and viewed by users outside of the United States,<sup>71</sup> and pro-Palestinian hashtags are older and more established than pro-Israeli hashtags.<sup>72</sup> In other words, the 10-to-1 statistic is not an accurate characterization of the videos posted and viewed on TikTok in the United States—and

---

<sup>68</sup> Ben Metzner, *Mitt Romney Reveals the Twisted Reason Why Congress Moved to Ban TikTok*, *The New Republic* (May 6, 2024), <https://perma.cc/VV6Y-QEYV> (quoting Senator Romney); Will Bunch, *Is TikTok Ban to Stop Kids Learning about Gaza?*, *Phila. Inquirer* (May 7, 2024), <https://perma.cc/3D2N-ERYL> (quoting Representative Lawler).

<sup>69</sup> David Ingram & Kat Tenbarger, *Critics Renew Calls for a TikTok Ban, Claiming Platform Has an Anti-Israel Bias* (Nov. 1, 2023), *NBC News*, <https://perma.cc/U2MW-BJSR>.

<sup>70</sup> *Id.*

<sup>71</sup> Louise Matsakis & J.D. Capelouto, *Asian & Middle Eastern Users Tilt TikTok Balance Toward Palestinians*, *Semafor* (Nov. 3, 2023), <https://perma.cc/U5BL-XVEF>.

<sup>72</sup> *The Truth about TikTok Hashtags and Content During the Israel-Hamas War*, *TikTok* (Nov. 13, 2023), <https://perma.cc/KE8G-98S2>; *see also* Paul Matzko, *Lies, Damned Lies, and Statistics: A Misleading Study Compares TikTok and Instagram*, *Cato Inst.* (Jan. 2, 2024), <https://perma.cc/KK77-HN2X> (criticizing study comparing the use of political hashtags on TikTok and Instagram insofar as the study failed to control for how long each platform existed and thus the time period over which certain political hashtags were used on each platform).

most importantly does not accurately describe data about what U.S. users were seeing—after the October 7 attacks.<sup>73</sup>

37. A review of U.S. hashtag data for the month after the October 7 attacks shows that only a slightly higher number of videos with pro-Palestinian hashtags were posted to the U.S. TikTok platform as compared to videos with pro-Israeli hashtags.<sup>74</sup> Moreover, the view counts for these sets of videos were roughly the same.<sup>75</sup> Indeed, an analysis by TikTok shows that videos with pro-Israeli hashtags received 68% more views per video in the United States than videos with pro-Palestinian hashtags.<sup>76</sup> And third-party analyses based on TikTok’s Research API—a data set comprised of public data that TikTok makes available to researchers—similarly show that videos with pro-Israeli hashtags and/or hashtags associated with content about the Israeli-Palestinian conflict that is neither pro-Israeli nor pro-Palestinian generally received more views per video in the weeks and months after the October 7 attacks as compared to videos with pro-Palestinian hashtags.<sup>77</sup> This suggests that, in general, videos posted with pro-Israeli hashtags received as many or more views per video on TikTok than videos with pro-Palestinian hashtags.<sup>78</sup> These statistics undercut the claim that TikTok is somehow “promoting” pro-Palestinian content on the app.

---

<sup>73</sup> It should also be noted that analyses based on hashtag data have certain limitations. For example, hashtags are assigned by users and do not always accurately reflect the subject matter of the videos to which they are assigned. Users may also post videos without hashtags.

<sup>74</sup> Ingram & Tenbarger, *supra* n.69.

<sup>75</sup> *Id.*; see also EJ Dickson, *Is TikTok Really Boosting Pro-Palestinian Content?*, Rolling Stone (Nov. 12, 2023), <https://perma.cc/K6NV-RXJ2>.

<sup>76</sup> *The Truth about TikTok Hashtags*, *supra* n.72.

<sup>77</sup> Laura Edelson, *Getting to Know the TikTok Research API*, Cybersecurity for Democracy (last accessed June 12, 2024), <https://perma.cc/V3AJ-8JEP>.

<sup>78</sup> Ingram & Tenbarger, *supra* n.69; Dickson, *supra* n.75.

38. Even if there were significantly more pro-Palestinian content on TikTok, the presence of such content does not demonstrate or in any manner prove that TikTok's recommendation algorithm is "promoting" a pro-Palestinian message. Rather, the prevalence of such content may simply be a function of the demographics of TikTok's user base, which trends younger than other platforms.<sup>79</sup> This is significant because recent polling shows that young people are less likely to support Israel's actions following the October 7 attacks as compared to older individuals, with one poll finding that only 20% of 18-to-24-year-olds support Israel's reaction to the attacks, as compared to 58% of respondents aged 50 years or older.<sup>80</sup> More broadly, the polling trends show that young people's support for Israel has been decreasing over the last 10 years—a trend that pre-dates TikTok's existence and even more so its widespread popularity.<sup>81</sup> In other words, the evidence does not support the conclusion that TikTok is the cause of young people's lower levels of support for Israel, as opposed to a reflection of pre-existing trends.<sup>82</sup>

---

<sup>79</sup> Monica Anderson Michelle Faverio & Jeffrey Gottfried, *Teens, Social Media & Technology 2023*, Pew Research Center (Dec. 11, 2023), <https://perma.cc/3PKM-NXAT> (finding that a greater percentage of teenagers use TikTok than any other social media application or entertainment platform, with the exception of YouTube); Rebecca Jennings, *TikTok Isn't Creating False Support for Palestine. It's Just Reflecting What's Already There.*, Vox (Dec. 13, 2023), <https://perma.cc/B5KE-KMQ8> (reporting that approximately 60% of TikTok's U.S. monthly active users are between 16 and 24 years old and another 26% are between 25 and 44 years old).

<sup>80</sup> *Sympathy Grows for Palestinians but Majority Still Sympathize More with Israelis, Quinnipiac University National Poll Finds; Generational Divide Widens on View of Israel*, Quinnipiac Univ. Poll (Nov. 16, 2023), <https://perma.cc/B7QS-FC67>.

<sup>81</sup> Lydia Saad, *Young Adults' Views on Middle East Changing Most*, Gallup (Mar. 24, 2023), <https://perma.cc/83J2-YD6U>.

<sup>82</sup> To the extent Members of Congress have cited the incidence of pro-Palestinian content on TikTok as compared to other platforms, *see, e.g.*, Metzner *supra* n.68, it is important to note that comparing the type and volume of content across different applications can be difficult, including because different platforms have different user numbers, serve different markets and



39. Certain Members of Congress have also cited the existence of videos on TikTok reciting, discussing, or reacting to Osama bin Laden’s “Letter to America” as a reason for voting in favor of the Act.<sup>83</sup> Content related to bin Laden’s letter, however, is not unique to TikTok. Other social media platforms saw increased engagement with bin Laden’s letter in the aftermath of the October 7 attacks, indicating that the letter presented an industry-wide issue.<sup>84</sup> The temporary virality of the letter may also be a function of a media “feedback loop” that is a familiar phenomenon of social media. According to public reports, engagement with TikTok videos regarding bin Laden’s letter increased dramatically only after media reports about the existence of such content on the app, suggesting that interest in the videos stemmed in substantial measure from media reports on other platforms about the existence of the videos as opposed to the popularity of such content on its own, let alone efforts by TikTok to promote or disseminate

---

demographics, and were founded at different times, *see* Matzko, *supra* n.72. Moreover, different platforms make different types of data publicly available. Even so, there are public reports that there is significantly more content with pro-Palestinian hashtags on Facebook and Instagram as compared to content with pro-Israeli hashtags. *See, e.g.*, Drew Harwell, *TikTok Was Slammed for Its Pro-Palestinian Hashtags. But It’s Not Alone*, Wash. Post. (Nov. 13, 2023), <https://perma.cc/6CYQ-GE3N> (reporting that, as of November 2023, there were 39 times as many posts on Facebook with the #freepalestine hashtag as compared to posts with the #standwithisrael hashtag; on Instagram, there were 26 times as many posts with the #freepalestine hashtag as compared to posts with the #standwithisrael hashtag).

<sup>83</sup> *See, e.g.*, Maheshwari *et al.*, *supra* n.54 (quoting Representative Krishnamoorthi). In his “Letter to America,” written in 2002, bin Laden purports to explain why al Qaeda attacked the United States on September 11, 2001. In doing so, bin Laden criticizes the U.S. government’s involvement in the Middle East and its support for Israel. *See* Bobby Allyn, *The Story Behind the Osama bin Laden Videos on TikTok*, NPR (Nov. 17, 2023), <https://perma.cc/U9FS-BY5E>.

<sup>84</sup> *See* Daysia Tolentino, *TikTok Removes Hashtag for Osama bin Laden’s “Letter to America” after Viral Videos Circulate*, NBC News (Nov. 16, 2023), <https://perma.cc/4BHH-48YL> (reporting a 4,300% increase in references to bin Laden on X between November 14 and 16, 2023, and a 400% increase in searches for bin Laden on YouTube over the same period).

such content.<sup>85</sup> The reported temporary virality of the letter may also have resulted from efforts by malicious actors to manipulate platforms' recommendation engines. Such conduct is a well-documented phenomenon that exists across many different platforms and is not limited to TikTok.<sup>86</sup>

40. Other Members of Congress have cited TikTok's March 2024 decision to display a pop-up message urging users to contact their representatives about the Act as a reason for voting in favor of the Act's provisions.<sup>87</sup> According to Representative Krishnamoorthi, TikTok's action "transformed a lot of lean yeses into hell yeses."<sup>88</sup> Here again, however, TikTok's actions do not distinguish TikTok from other companies and, in fact, reflect industry-wide practices. In response to a proposal by then-New York City Mayor Bill de Blasio to restrict the number of Uber drivers allowed to operate in New York City, Uber added an option on its app that allowed users to select a "DE BLASIO" ride, which Uber suggested would resemble the app experience if Mayor de Blasio's measure passed.<sup>89</sup> Among other things, the "DE BLASIO" option informed users that their ride would arrive in 25 minutes.<sup>90</sup> In 2012, Google displayed a blacked-out logo on its homepage along with a message directing users to "Tell Congress: Please don't censor the

---

<sup>85</sup> Drew Harwell & Victoria Bisset, *How Osama bin Laden's "Letter to America" Reached Millions Online*, Wash. Post (Nov. 16, 2023), <https://perma.cc/29VS-QBML>.

<sup>86</sup> Christian Kastner, *Security and Privacy in ML-Enabled Systems*, Medium (Dec. 20, 2022), <https://perma.cc/9BNW-2JAF>.

<sup>87</sup> Sapna Maheshwari, David McCabe & Cecilia Kang, "*Thunder Run*": Behind Lawmakers' Secretive Push to Pass the TikTok Bill, N.Y. Times (Apr. 24, 2024), <https://perma.cc/BR72-P779> (quoting Representative Krishnamoorthi).

<sup>88</sup> *Id.*

<sup>89</sup> Christopher Spata, *Uber Slams NYC Mayor with New "DE BLASIO" Feature*, Complex (Jul. 16, 2015), <https://perma.cc/T3ZQ-SRUS>.

<sup>90</sup> *Id.*

Web.”<sup>91</sup> Google’s temporary change to its homepage responded to certain legislation pending in Congress at the time, which Google believed would “impose huge regulatory costs and stifle innovation on the Web.”<sup>92</sup> Such actions are not materially different from TikTok’s asserted efforts to mobilize its user base in response to the Act’s introduction. In each instance, it was left to users whether to engage in the democratic activity of contacting their representatives.

41. Finally, it bears mention that the Act’s treatment of TikTok stands in contrast to its treatment of foreign-owned news applications, including applications owned by Xinhua News (China), RT News (Russia), and NewsBreak (China), that operate in the United States.<sup>93</sup> RT News has been publicly identified by the U.S. Department of State as “play[ing] an important role within Russia’s disinformation ecosystem” and, according to the Department of State, serves as a “conduit[] for Kremlin talking points aimed at influencing foreign public opinion in a way that benefits Russia’s foreign policy and national security interests.”<sup>94</sup> Xinhua News, in turn, has been described as the “world’s biggest propaganda agency,”<sup>95</sup> with the U.S. State Department characterizing Xinhua as a “PRC [People’s Republic of China] propaganda outlet[.]”<sup>96</sup> And

---

<sup>91</sup> Michael Cavanaugh, *Google Blacks Out: “Censored” Logo Goes Dark to Oppose SOPA/PIPA Legislation*, Wash. Post (Jan. 18, 2012), <https://perma.cc/V69T-NJGZ>.

<sup>92</sup> *Id.*

<sup>93</sup> See Xinhua News (last accessed June 12, 2024), <https://perma.cc/W4X3-X9GV>; RT News (last accessed June 12, 2024), <https://perma.cc/F4FX-2KE9>; James Pearson, *NewsBreak: Most Downloaded U.S. News App Has Chinese Roots and ‘Writes Fiction’ Using A.I.*, Reuters (June 5, 2024), <https://perma.cc/EE28-NC8C>.

<sup>94</sup> *Kremlin-Funded Media: RT and Sputnik’s Role in Russia’s Disinformation and Propaganda Ecosystem*, U.S. Dep’t of State Global Engagement Ctr. (Jan. 2022), <https://perma.cc/S9ES-G5GL>.

<sup>95</sup> *Xinhua: The World’s Biggest Propaganda Agency*, Reporters Without Borders (Oct. 2005), <https://perma.cc/UGB9-M4ES>.

<sup>96</sup> *Designation of Additional Chinese Media Entities as Foreign Missions*, U.S. Dep’t of State (June 22, 2020), <https://perma.cc/VJS6-5JE6>.

recent reports state that NewsBreak—a subsidiary of a “Chinese news aggregation app” with a China-based engineering team—has become a popular news app in the United States, notwithstanding claims that the app routinely publishes fictitious news stories on its platform.<sup>97</sup> From a national security perspective, there is no reason to apply one set of rules to applications owned by or affiliated with ByteDance (including TikTok) and another set of rules to applications owned by or affiliated with RT News, Xinhua News, NewsBreak, and similar companies.

### III. Conclusion

42. Social media and entertainment platforms, like TikTok, raise important policy issues, including the appropriate protection of user data, content moderation, and propaganda. These are legitimate issues to consider from a policy perspective, but they are issues that the industry confronts as a whole and are not unique or distinctive to TikTok.

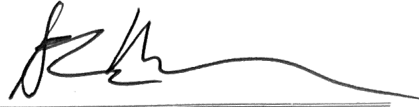
43. As I have discussed above, TikTok’s approach for dealing with these issues is in line with—and in many respects markedly better than—industry best practices, even for companies that hold significant sensitive user data. In light of the foregoing, there is no evident national security rationale for the Act’s particular focus on TikTok. It is arbitrary to select one market participant for policy issues that an entire industry faces. This is particularly the case where there exist alternative mechanisms—including the mitigation proposals that TikTok Inc. has outlined in the NSA negotiated with CFIUS—that enable the federal government to use regulatory frameworks and establish extensive processes that mitigate data and national security risks around data and algorithms beyond what they would currently be able to achieve with peer firms.

---

<sup>97</sup> Pearson, *supra* n.93.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 17th day of June, 2024.



Steven Weber

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

<hr/>		)
TIKTOK INC.		)
		)
and		)
		)
BYTEDANCE LTD.,		)
		)
	<i>Petitioners,</i>	)
		)
v.		)
		)
		)
		)
MERRICK B. GARLAND, in his		)
official capacity as Attorney General		)
of the United States,		)
		)
	<i>Respondent.</i>	)
<hr/>		)

No. 24-1113

**DECLARATION OF ADAM PRESSER**

1. I am TikTok’s Head of Operations and Trust & Safety, a role I have served in since March 2024, and I am employed by Petitioner TikTok Inc. Between June 2023 and March 2024, I was TikTok’s Head of Operations, and before that, from April 2022 to June 2023, I was Vice President and TikTok Chief of Staff. As Head of Operations and Trust & Safety, my responsibilities include cultivating, maintaining and protecting TikTok’s global content ecosystem. The teams I lead manage

our content operations and distribution all over the world, as well as our efforts to identify and remove harmful content on the platform globally. As a senior executive, I have also become broadly familiar with our operations and policies across a range of areas, including TikTok's data privacy and security policies, engineering operations, and our engagement with stakeholders and regulators in the United States and abroad.

2. I am a U.S. citizen born and raised in Los Angeles, California. I have a B.A. and M.A. from Yale University, a J.D. from Harvard Law School, and an MBA from Harvard Business School. Before I joined TikTok, I worked for Warner Bros. Entertainment and then WarnerMedia, most recently as Executive Vice President, International and Head of WarnerMedia China, Australia and New Zealand, and Head of WarnerMedia International Home Entertainment Licensing. I have extensive experience working in multinational business operations in a variety of structures, including with joint ventures, licensing partners, and, as with TikTok, globally integrated businesses.

3. The purpose of this declaration is to provide an overview of the TikTok platform, including how we protect U.S. users' data and guard against foreign government influence. I also explain why the U.S. TikTok platform cannot realistically be severed from the rest of the global platform in one year, as I understand would be required to avoid a ban of TikTok under the "Protecting Americans from Foreign Adversary Controlled Applications Act."

**I. Background on Petitioners TikTok Inc. and ByteDance Ltd.**

4. Like many global businesses, TikTok operates through multiple corporate entities. 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. References in my declaration to "TikTok Inc." are to this specific corporate entity; references to "TikTok" are to the online platform.

5. TikTok Inc.'s ultimate parent company is ByteDance Ltd., a Cayman Islands-incorporated equity holding company that has multiple operating subsidiaries, including in China. References in my



declaration to “ByteDance Ltd.” are to this specific corporate entity, whereas more general references to “ByteDance” are to the corporate group, including its operating subsidiaries. ByteDance was founded in 2012 by two Chinese engineers. Today, approximately 58 percent of ByteDance Ltd. is owned by global institutional investors, including General Atlantic and Susquehanna International Group; 21 percent is owned by its global employee workforce; and 21 percent is owned by one of its founders, Zhang Yiming (a Chinese national who lives in Singapore).

6. In addition to TikTok Inc., which provides the TikTok platform in the United States, other subsidiaries of ByteDance Ltd. provide several other applications, services, and online platforms in the United States, including for content sharing, video and music editing (such as the popular video-editing app CapCut), e-commerce, gaming, and enterprise productivity.

## **II. The TikTok Platform**

7. TikTok is an online platform that enables users to create, share, and view videos. TikTok’s mission is “to inspire creativity and

bring joy,”<sup>1</sup> and we seek to bring this mission to life through the products we build, the content we cultivate and recommend, and the rules we publish and enforce to keep harmful content away from our users.

8. TikTok is designed to provide a creative and entertaining forum for our users to express themselves and make connections with other content creators and viewers. TikTok users primarily engage with the platform by creating and sharing videos or by watching and interacting with videos posted by others. In addition to sharing and commenting on videos, users can connect with one another in a variety of other ways, including “tagging” other users in the comments, using the app’s “duet” and “stitch” tools to create new content that incorporates and responds to content created by others, using the “TikTok LIVE” feature to communicate live with others on the platform, and sending direct messages to one another. The TikTok platform is offered in more than 170 countries, but it is not offered in mainland China.

---

<sup>1</sup> Our Mission, TikTok, [https://www.tiktok.com/about?lang\\_en](https://www.tiktok.com/about?lang_en) (last visited June 17, 2024).

9. TikTok is a globally integrated platform, meaning that content posted in one country is generally available to users in any of the 170+ countries in which TikTok is available. There is an enormous array of international content available to U.S. users on the platform, some of which is extremely popular. Just to take a few examples, there is content about global sporting events like the Olympic Games (@olympics has 8.3 million followers), international sports teams (@realmadrid has 45.5 million followers), and international music such as K-pop (one of the most popular groups, BTS, has 65.3 million followers) and Tomorrowland, an annual music festival in Ibiza, Spain (@tomorrowland has 5.7 million followers).

10. TikTok was first launched globally in May 2017 in over 150 countries, including the United States. After ByteDance Ltd. acquired another short-form video platform, musical.ly, and moved its user base to TikTok, TikTok was re-launched in the United States in August 2018.

11. Since then, TikTok has grown to become one of the most widely used online platforms in the world. TikTok has more than 170 million monthly users in the United States and more than 1 billion

users worldwide. With so many U.S. users, the volume of content created and viewed in the United States is correspondingly immense. In 2023, TikTok users in the United States uploaded more than 5.5 billion videos, which were viewed more than 13 trillion times here and abroad; half of those video views came from users outside the United States. In the same year, TikTok users in the United States viewed content from outside the United States more than 2.7 trillion times, which accounted for more than a quarter of all video views in the United States. U.S. content is also disproportionately popular abroad; for example, last year, even in several of TikTok’s non-U.S. English-speaking markets, content from the United States comprised more than a third of all video views.

12. TikTok’s initial growth was spurred by its appeal to those who value the blend of light entertainment and humor our platform provides. Today, TikTok also has become a forum for all types of speech, including about politics, sports, family, religion, and users’ jobs and hobbies.<sup>2</sup> Many content creators use our platform to express their

---

<sup>2</sup> TikTok does not, however, permit paid political advertising on the platform. *See* TikTok Business Help Center, Ad Policy Handbook: North

opinions, share their stories, support their preferred political candidates, and speak out on today's many pressing issues, all to a global audience of more than one billion monthly users.

13. TikTok Inc. itself maintains an active account on TikTok, operated by a U.S.-based team, which has more than 80 million followers globally. 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. The company also interacts with users by promoting public-interest content on TikTok, such as our "EduTok" campaign, which encourages users to create and share educational and motivational content on a variety of themes. The company has also launched other campaigns to promote public interest content. TikTok users also have the ability to use special filters, special effects, and stickers available on the platform to enhance their content and express their views on issues of public interest.

---

America (last updated June 2024),  
<https://ads.tiktok.com/help/article/ad-policy-handbook-north-america>.

14. Although there are other platforms that allow users to post and share content, TikTok differs from these platforms in important respects. For example, unlike other platforms, TikTok does not host written posts (except insofar as a user posts a video or picture showing written text), and it is not as focused on users' interactions with existing friends, family, or co-workers, like some other platforms are.

15. Instead, the TikTok experience is centered on discovering video content primarily through the app's For You feed, which opens a collection of videos curated by TikTok's proprietary recommendation engine based on an individual user's interests and how the user interacts with content they watch. With the For You feed, TikTok's focus is on facilitating users' discovery and exploration of new content and new communities that might be of interest to them. The For You feed provides individual, regular TikTok users a unique ability to discover new content and, for those who choose to post their own content, to reach a new and broader audience. The For You feed (and its recommendation engine) is central to the TikTok experience and one of the defining features of the TikTok platform that made it successful.

16. Although the For You feed is the most popular way users use TikTok, users can explore content on TikTok in a variety of other ways. For example, users can use the search function to find content about particular topics they are interested in. Videos in search results are sorted according to a combination of factors, including relevance to a user's search query and other users' level of engagement with the video. Relevance is determined based on things like video captions, video text, and "hashtags," all of which can only be added by the users themselves upon uploading the videos.

17. On TikTok and other online platforms, hashtags function as content aggregators, which means that a user can locate other content with that hashtag by searching for the hashtag or clicking on the hashtag in a comment or video caption. Hashtags help users to find content that appeals to their particular hobbies, athletic pursuits, or identities and to connect with others, including through #booktok (33.8 million posts), #baseball (4.3 million posts), #blacktiktok (4.7 million posts), and #fitness (37.8 million posts). Many creators also use the platform to post product reviews, business reviews, and travel

information and reviews. For example, #travel has 46.1 million posts on TikTok.

18. Because a significant percentage of videos posted on TikTok do not have any hashtags at all, hashtags will rarely capture all of the content associated with a specific topic. For that reason, the platform's search function is based on a number of inputs, not just hashtags. For example, while #taylorswift is associated with 13.2 million posts on TikTok, a search for the term "Taylor Swift" would generate many more posts. For the same reason, it is not possible to compare the prevalence of different kinds of content on TikTok, or make comparisons to other platforms, by looking only at hashtag numbers. Through our Research Tools, qualifying researchers in the U.S. and Europe can apply to study public data about TikTok content and accounts.

19. Users can also view a feed consisting only of content posted by those creators they have decided to "follow." That allows users to curate their own viewing experience, rather than only relying on TikTok to do so.

20. Creators come to TikTok because of the platform's unique attributes. In my experience, creators join TikTok because of its ability



to facilitate discovery through organic reach—that is, the number of people who see a post through unpaid distribution. TikTok’s organic reach allows creators to reach large numbers of users—beyond their current universe of followers—without any paid promotion. Moreover, TikTok’s recommendation system facilitates users’ access to content created by a wide range of individuals, meaning that it is not unusual for videos created by regular people to “go viral” and receive thousands, if not millions, of views. Many platforms offer creators a forum to reach new audiences. But TikTok is unique in its ability to generate reach for regular people. For example, nine of the top ten TikTok accounts with the most followers were regular people before they joined the platform and started posting, and the tenth account is TikTok’s own account. By comparison, for several of our competitors, the most-followed accounts belong to people who are independently famous, like athletes, actors, and musicians.

### **III. The Content Available on the TikTok Platform**

21. We always strive to show our users content that serves our mission to “inspire creativity and bring joy” in a safe environment. In service of that goal, we use three main editorial processes to determine

what content is shown to users: content moderation, content recommendation, and video promotion and filtering.

A. Content Moderation

22. The first process that determines the content available to users is content moderation. As noted above, I oversee the TikTok Trust & Safety team, which is responsible for content moderation globally. This year, we anticipate spending more than \$2 billion on Trust & Safety globally, and the TikTok Trust & Safety team I oversee includes more than 40,000 employees and contractors worldwide.

23. Consistent with our guiding principle to enable free expression while preventing harm, the goal of content moderation is to create a welcoming and safe experience for our users. The content moderation process applies to all content available on the platform, whether viewed on the For You feed or discovered via searching.

24. Our approach to content moderation is built on the foundation of our Community Guidelines, a publicly available collection of rules and standards that apply to all TikTok users and content.<sup>3</sup> The

---

<sup>3</sup> *Community Guidelines*, TikTok (last updated April 17, 2024), <https://www.tiktok.com/community-guidelines?lang=en>.

team that writes the Community Guidelines reports to me, and I ultimately approve the Community Guidelines before they are published on the platform and our website. The Community Guidelines were created and are continually refined in consultation with third-party experts, including our U.S. Content Advisory Council. The Content Advisory Council brings together groups of American independent experts who help us develop forward-looking policies and processes to help create a safe platform for everyone. They work with us to inform and strengthen our policies, product features, and safety processes.

25. The Community Guidelines include rules for what is allowed on TikTok, as well as standards for what content is eligible for recommendation to users in the For You feed. Among other things, the Community Guidelines prohibit nudity; promotion of or incitement to violence; promotion of criminal activities that may harm people, animals, or property; hate speech, hateful ideology, and hateful behaviors; promotion of violent or hateful political organizations; animal abuse; and harassment and bullying. Of course, on a platform as large as ours, it is natural for people to have different opinions, and we

welcome that, but we do not allow influence operations, where networks of accounts work together to mislead people or our systems and try to strategically influence public discussion. The Community Guidelines also outline our policies for dealing with misinformation. And we also have a publicly disclosed policy regarding State-Affiliated Media.

26. We proactively enforce our Community Guidelines through a mix of technology-based and human moderation. Every video uploaded to TikTok goes through automated moderation before it appears on the platform so that content flagged as potentially violative can be automatically removed or escalated for human review by trained moderators. More than 75% of all videos removed for violating the Community Guidelines are never viewed by a single user. We also encourage users to take advantage of various tools provided through the app or on the website to report content that they believe violates the Community Guidelines. If we identify violative content—on our own or through our users—we remove such content from the platform. The team responsible for enforcing the Community Guidelines globally also reports to me. This team is governed by strict company-wide policies intended to ensure that content is moderated in accordance with our

Community Guidelines, and we enforce these policies with measures to track and audit moderation decisions.

27. In total, over 176 million videos were removed from TikTok in the period of October through December 2023 for violating the Community Guidelines. We publicly disclose these and other statistics regarding our enforcement of the Community Guidelines in our quarterly Community Guidelines Enforcement reports, which are posted on our website.<sup>4</sup> We also publish a report with information about covert influence operations we disrupt, including how they were detected, how many accounts we removed, how many followers the accounts had, and a description of the operations, including where it was operating from and the country that was targeted.<sup>5</sup> In addition to our transparency reports, as I mentioned above, through our Research Tools, qualifying researchers in the U.S. and Europe can apply to study public data about TikTok content and accounts, which provides additional transparency into the activity on our platform.

---

<sup>4</sup> *Community Guidelines Enforcement Report*, TikTok (published Mar. 19, 2024), <https://www.tiktok.com/transparency/en/community-guidelines-enforcement/>.

<sup>5</sup> *Covert Influence Operations Report*, TikTok, <https://www.tiktok.com/transparency/en/covert-influence-operations/>.

28. Even if content does not violate our Community Guidelines, we take steps as part of our content moderation processes to limit access to content that may not be suitable for certain users. For example, even though it may not violate the Guidelines, content depicting consumption of excessive amounts of alcohol by adults is not eligible for recommendation in the For You feed. Additionally, videos that some users may find to be distressing but that involve a subject of important public interest, are instead covered by “opt-in viewing screens” when flagged. These opt-in screens warn the user that the video may contain sensitive material and give the user the option to either view the content or skip to the next video.<sup>6</sup> Such videos are also ineligible for recommendation on users’ For You feeds.<sup>7</sup>

#### B. Content Recommendation

29. The second process we use to determine what content to show to users is content recommendation. Content recommendation is

---

<sup>6</sup> Cormac Keenan, Refreshing Our Policies to Support Community Well-Being, TikTok (Dec. 15, 2020), <https://newsroom.tiktok.com/en-us/refreshing-our-policies-to-support-community-well-being>; Tara Wadhwa, New Resources to Support Our Community’s Well-Being, TikTok (Sept. 14, 2021), <https://newsroom.tiktok.com/en-us/new-resources-to-support-well-being>.

<sup>7</sup> Keenan, *supra* n.6; Wadhwa, *supra* n.6.

implemented by TikTok's recommendation engine, a sorting and ranking mechanism that uses statistical modeling to select videos for a user's For You feed.

30. The recommendation system analyzes various signals from the user and other users, such as their likes, comments, and what they watch. The recommendation engine identifies a pool of candidate videos for a user, then scores and ranks those videos using machine-learning models that seek to determine which video would be most interesting to the user. As I described above, certain content is not eligible for recommendation in the For You feed and this content is not part of the candidate pool. To evaluate whether a user would find a particular video interesting, these models assign different weights to a variety of factors, including user engagement or activity information (such as video playtime, likes, shares, accounts followed, comments, content created), account or device information (such as language preference, country setting, device type), and video information (such as captions, sounds, hashtags). The system may adjust the weight assigned to a particular parameter if it "learns" that it is more or less important than

other factors in determining whether users are, or a particular user is, likely to engage with a given video.

31. In essence, the recommendation engine functions as a large matching system, matching users with content they are predicted to like based on their viewing habits.

32. The source code for TikTok's recommendation engine was originally developed by ByteDance engineers based in China and is continually developed by the TikTok Global Engineering Team. The recommendation engine is customized for TikTok's various global markets, including in the United States, and that customization is subject to special vetting in the United States. In addition to those protections, which I describe below, as with other source code, we have technical measures in place intended to ensure that only employees with appropriate access controls are able to update the recommendation engine, and those updates are also auditable.

### C. Video Promotion and Filtering

33. Video promotion and filtering is the third process determining what content is shown to users, and is similarly intended to ensure that users have a positive experience with content they enjoy.



We may promote specific content (e.g., highlights from the Super Bowl, or videos from a Beyoncé concert) in line with company content policies, including to support the inclusion of diverse and high-quality content on the platform.

34. Our internal policies strictly limit which employees can request promotion of content. Each request to promote a video is manually reviewed and either approved or rejected based on an assessment of whether it follows the platform's content policies, including to support content diversity and quality (for example, being engaging and meaningful and focusing on timely/relevant content) and business objectives. Each video that is promoted is reviewed at least once by a human reviewer, and these teams are regionalized, so all videos promoted in the U.S. are reviewed by a U.S.-based reviewer. Our global security teams also audit promotion requests to ensure that they are consistent with our policies. Promotion currently impacts less than 1% of video views in the United States.

35. Just as we promote certain specific content to improve the user experience, we also apply a set of rules to filter out and disperse certain content, i.e., not show one video after another about the same

subject, in users' For You feeds. The objective of filtering content is to make the platform safer and more enjoyable for our users and to support commercial and product goals such as prioritizing content from the same country, avoiding duplication, and ensuring appropriate video length. For example, we filter out from users' For You feed content that is predicted to be low quality (e.g., extremely short videos). We also disperse content to try to ensure sufficient diversity of content in a user's For You feed.

36. We also attempt to identify and disperse content that, viewed sparingly, is not harmful, but viewed repeatedly could be problematic, such as content about exercise, dieting, or mental health. These videos may be eligible for the For You feed, but, to protect our community, we work to interrupt repetitive patterns to ensure they are not viewed too often.

#### **IV. TikTok's Efforts to Safeguard U.S. User Data and the Integrity of the Platform Against Foreign Government Influence.**

37. TikTok has undertaken unprecedented efforts to safeguard U.S. user data and protect the integrity of the platform against foreign government influence.

38. Like other platforms, TikTok collects certain information from users in accordance with its Privacy Policy and Terms of Service, to which users must agree as a condition of signing up for the app.<sup>8</sup> Pursuant to the Privacy Policy, TikTok collects users' usernames, dates of birth, and, depending on how they sign up for the app, a user's phone number or email address.<sup>9</sup> Notably, however, there are also several categories of data that we do not collect. Unlike other platforms, for example, TikTok does not require its users to provide certain types of personal identifying information, such as the user's real name, employment information, or familial relationships or relationship status. The current version of the TikTok app also does not collect GPS information from U.S. users.

39. Starting in 2019, the U.S. government expressed concerns that the Chinese government could obtain access to user data TikTok collects from U.S. users, or compel ByteDance to manipulate the TikTok

---

<sup>8</sup> *Privacy Policy*, TikTok (last updated March 28, 2024), <https://www.tiktok.com/legal/page/us/privacy-policy/en>; *see also Terms of Service*, TikTok (last updated November 2023), <https://www.tiktok.com/legal/page/us/terms-of-service/en>.

<sup>9</sup> *Privacy Policy*, TikTok (last updated March 28, 2024), <https://www.tiktok.com/legal/page/us/privacy-policy/en>.

platform to promote the Chinese government's agenda in the United States. We disagree that these concerns are well-founded, but made a voluntary decision to engage for several years with the Committee on Foreign Investment in the United States on how to address those concerns. Following extensive engagement and the incorporation of significant U.S. government feedback, that process culminated in a 90-page draft National Security Agreement, the latest draft of which we provided to the government on August 23, 2022.

40. The full range of commitments is described in the draft National Security Agreement, but in summary it contains several layers of protections that would enable the U.S. government to validate the security of U.S. user data and confirm that the platform is free from improper influence by any foreign government. To our knowledge, no other online platform provides these kinds of protections, which even include a "shut-down option" that would give the government the authority to suspend TikTok in the United States if we violate certain obligations under the agreement. These protections are in addition to our existing policy, technical, and transparency safeguards

implemented on a global basis to safeguard TikTok user data and protect the integrity of the platform against foreign interference.

41. Although the draft National Security Agreement was never signed, we have voluntarily begun implementing many measures that do not require the U.S. government's cooperation. We have invested more than \$2 billion on that effort—sometimes referred to as “Project Texas.” Among the steps we have taken as part of this initiative are the following:

42. Independent Governance. We have created a special purpose subsidiary of TikTok Inc. called TikTok U.S. Data Security Inc. (“TikTok USDS”) to control access to protected U.S. user data (as defined in our draft National Security Agreement) and monitor the security of the platform. The TikTok USDS team is currently led by Interim General Manager Andy Bonillo and Interim Security Officer Will Farrell, both of whom are U.S. citizens with significant experience working with the U.S. government on national security and cybersecurity matters. All TikTok USDS employees, of which there are now over 2,000, report to Mr. Bonillo and Mr. Farrell. TikTok USDS

employees work in offices that are physically separate from that of other TikTok or ByteDance personnel.<sup>10</sup>

43. Data Protection and Access Controls. We have partnered with Oracle Corporation on the migration of the U.S. platform and protected U.S. user data to Oracle's cloud environment. Every U.S. user now interacts with a version of TikTok that is run in the Oracle environment, and we have taken steps to store protected U.S. user data there. Access to the Oracle environment is limited to only TikTok USDS personnel, unless authorization is given by TikTok USDS pursuant to limited exceptions, such as for legal and compliance purposes.

44. Software Assurance. TikTok USDS and Oracle review updates to the U.S. TikTok app developed by employees outside TikTok USDS, and all software updates are deployed, i.e., implemented on the U.S. TikTok platform, by TikTok USDS personnel. TikTok USDS also reviews changes to the platform code base, and Oracle has full access to

---

<sup>10</sup> The draft National Security Agreement requires TikTok USDS to be governed by an independent board with Security Directors whose appointment would be subject to the U.S. government's approval and would exclude ByteDance and its subsidiaries and affiliates from any oversight of TikTok USDS. TikTok USDS has provided nominees for these directors to the U.S. government, but the government has not yet approved them.

review the entire source code, including any updates, in dedicated transparency centers located in Columbia, Maryland; Denver, Colorado; the United Kingdom; and Australia.

45. Content Assurance. TikTok's U.S. recommendation engine is stored in the Oracle cloud. TikTok USDS now deploys the recommendation engine in the United States, and as noted above, Oracle has full access to review the entire TikTok platform source code, which includes the algorithm for the recommendation engine. TikTok USDS also reviews and approves content promotion requests to help ensure that content promotion on the U.S. TikTok platform is conducted consistently with our policies and is free of foreign-government interference.

#### **V. The Prohibitions in the Act Will Lead to TikTok Being Inoperable in the United States.**

46. As I understand it, the Act contains two types of prohibitions. First, it prohibits "services to distribute, maintain, or update" the TikTok platform in the United States "by means of a marketplace (including an online mobile application store)." Second, it prohibits "internet hosting services to enable the distribution, maintenance, or updating of" the TikTok platform. Together, these

prohibitions would render the TikTok platform inoperable in the United States.

47. With respect to the first prohibition, removing the app from U.S. app stores will halt the influx of any new U.S. users, immediately foreclosing millions of Americans who have not yet downloaded the app from joining TikTok.

48. Even those users and creators who choose to stay on the platform would be affected by the removal of the TikTok app from app stores. We also regularly update the software for the TikTok app, and consumers receive those updates via app store downloads. This prohibition would accordingly prevent users from downloading updates to the app, including security fixes. The inability to download updates would eventually render the app incompatible with the TikTok platform and therefore inoperable.

49. The second prohibition, on the provision of internet hosting services, would likewise prevent us and our commercial partners from providing the services that enable the TikTok platform to function, effectively shutting down TikTok in the United States. For example, internet service providers may stop routing traffic to TikTok.com; data



centers may not renew contracts because it would be unclear if they would be allowed to host TikTok code, content, or data; and content delivery networks (“CDNs”) that are spread throughout the country may also be covered. The termination of these services would cripple the platform in the United States and make it totally unusable.

50. Even a temporary implementation of these prohibitions would cause significant and irreversible harms to our business and our brand. Users and content creators tend to develop lasting brand loyalty when it comes to social media and online entertainment platforms, and if we lose these users and content creators to our competitors, even on a temporary basis, some are not likely to return, even if the prohibitions are later lifted. Accordingly, even if the prohibitions of the Act are later lifted, we would not be able to make up for lost ground, because people who would have downloaded TikTok will have already turned to other competing platforms.

51. The prohibitions also would dramatically undercut the commercial goodwill associated with TikTok and impede our ability to form and maintain commercial partnerships. By destroying the vibrant TikTok community in the U.S., the prohibitions will deal a heavy blow

to our reputation and attractiveness as a commercial partner. This collapse of goodwill will harm our revenues from existing partnerships and prevent us from realizing revenue from future opportunities, as prospective partners forge relationships with our competitors instead. If we are perceived to be an unreliable partner in the marketplace, advertisers will build partnerships with other platforms.

52. Being banned from the United States will also devastate our U.S. workforce, permanently harming our ability to recruit and retain talent. TikTok is a technology company, and we compete fiercely for the software engineers and other talent we rely upon to run our business. These candidates often have multiple offers from other companies. Since the Act was signed into law, our competitors have been aggressively trying to recruit our talent. As the prohibitions come into effect, these problems with recruitment and retention will be greatly magnified, given that the business these employees support would be banned in the United States.

## **VI. Severing the U.S. TikTok Platform from ByteDance and the Global TikTok Platform.**

53. I understand that the only way to avoid those prohibitions is if the U.S. TikTok platform is sold, leaving no subsequent operational

relationship with the rest of the global TikTok platform or the ByteDance affiliate employees that currently support it.

54. As discussed above, TikTok in the United States is an integrated part of the global TikTok platform. The global TikTok business is led by a leadership team based in Singapore and the United States. Many of the teams that support the global TikTok platform, including engineering, operations, Trust & Safety, and advertising sales, are spread across several different corporate entities and countries.

55. Because the platform and the content is global, the teams working on the platform, and the tools they use, necessarily must be, as well. For example, as I mentioned above, we do not allow animal abuse on the platform, and we use software tools to identify content depicting animal abuse. It is important that the tools used to automatically detect animal abuse are effective and consistent. We have accordingly developed and refined those tools at the global level, drawing on resources from multiple functions in different countries.

56. As another example, several members of my senior leadership team are based outside the United States, including in

London, Dublin, and Singapore, and they are responsible for a wide range of global functions on our Operations and Trust & Safety teams, including managing all content moderators globally, overseeing global publisher relationships, working with law enforcement authorities around the world to prevent crimes on the platform, and managing copyright takedown requests.

57. The global TikTok platform also relies on the support of employees of other ByteDance subsidiaries for some functions, including the development of portions of the computer code that runs the TikTok platform. These integrated relationships are consistent with our commitments under Project Texas, pursuant to which TikTok USDS and Oracle vet updates to the U.S. platform developed by engineers outside TikTok USDS. In other words, Project Texas contemplates that source code supporting the TikTok platform, including the recommendation engine, will continue to be developed and maintained by ByteDance subsidiary employees, including in the United States and in China, and that any such source code is reviewed and vetted by TikTok USDS and Oracle.

58. Given these integrated relationships, there are several reasons why a severance of the U.S. TikTok platform from the rest of the globally integrated TikTok platform and business is not feasible.

59. First, as I have mentioned, TikTok is a globally integrated online platform where content created in one place is generally available everywhere else. The same is true of TikTok's competitors in the United States, like YouTube, Instagram, and Snapchat. For example, as mentioned above, in 2023, half of views of videos posted in the United States came from users outside the United States, and non-U.S. content accounted for more than a quarter of all video views in the United States.

60. Divesting the U.S. TikTok business in a way that precludes any further operational relationship with the rest of TikTok outside the United States would prevent international content from being seamlessly available in the U.S. market and vice versa. I understand that, to avoid a ban, the Act requires divestment of the U.S. TikTok application, without any ongoing operational relationship with non-U.S. TikTok or ByteDance entities, including any agreement to share user data. In the absence of an operational relationship, including an

agreement to share content and data with the entities that operate the global platform, the U.S. TikTok platform would become an “island” where Americans would have an experience isolated from the rest of the global platform. U.S. users on a U.S.-only version of TikTok would be unable to access the content posted by any non-U.S. TikTok users, and U.S. creators would be unable to reach that audience abroad.

61. Such a U.S.-only version of TikTok would be unable to compete with rival, global platforms. The rich pool of global content on the TikTok platform helps generate more users and more traffic, which in turn attracts more (and more popular) creators, which in turn attracts more user traffic, restarting the cycle. Our ability to attract advertisers and drive revenue depends on user engagement. A platform of exclusively American users will be significantly less attractive to global advertisers and creators than a rival platform operating on a global scale, leading to the reverse of the cycle I described above.

62. The operational costs associated with running an online platform for user-generated content, including the extensive Trust & Safety and content assurance operations I have described above, could not be sustained by a purely U.S.-only platform. For example, I

mentioned above that we will spend over \$2 billion on Trust & Safety this year. A U.S.-only platform would likely incur many of the same expenses, including on technology tools and third-party safety experts, because those costs are largely independent of the number of users on the platform and instead are mainly fixed costs associated with continually refining and maintaining a complicated set of technological and human systems and processes for a large platform hosting user-generated content. But while the costs for a U.S.-only platform would be on the same scale as they are currently, the base of revenue to support them would be considerably smaller.

63. Second, setting aside these commercial dynamics, divesting the U.S. TikTok platform in the manner and on the timeline required by the Act would not be technologically feasible because it would require the U.S. platform to be severed from the ByteDance engineers responsible for maintaining and updating its code base.

64. The code base supporting the TikTok platform includes billions of lines of code that have been developed over multiple years by a team of thousands of global engineers, including in China. To complete a divestiture required by the Act, *none* of those thousands of

ByteDance employees would be permitted to continue to support TikTok in the United States. Under those circumstances, there is no question that it would take at least several 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. Even then, such a newly-created team of engineers would need access to custom-made ByteDance software tools, which the Act prohibits.

65. As I mentioned above, during my time at WarnerMedia and most recently at TikTok, I have worked to implement a variety of corporate relationships and reorganizations, including licensing agreements, joint ventures, mergers, and spin-offs. The divestiture contemplated by the Act is fundamentally different—a sale within one year without any possibility of follow-on cooperation. Such a transaction for a platform of TikTok’s size and scope is infeasible along the timeline dictated by the Act.



Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this day June 17, 2024.

  
\_\_\_\_\_  
Adam Presser