

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

---

TIKTOK INC., *et al.*, )  
 )  
 )  
 Plaintiffs, )  
 )  
 v. )  
 )  
 DONALD J. TRUMP, in his official capacity as )  
 President of the United States, *et al.*, )  
 )  
 Defendants. )  


---

Civil Action No. 1:20-CV-2658-CJN

**REDACTED – ORIGINAL FILED  
UNDER SEAL**

**DEFENDANTS’ MEMORANDUM IN OPPOSITION TO PLAINTIFFS’ MOTION FOR A  
PRELIMINARY INJUNCTION**

**TABLE OF CONTENTS**

Introduction..... 1

Background..... 2

I. Statutory Framework ..... 2

    A. The International Emergency Economic Powers Act ..... 2

    B. The National Emergencies Act ..... 3

II. Factual Background on the PRC, ByteDance, and TikTok..... 4

    A. The PRC Is a Significant and Growing National Security Threat ..... 5

    B. Chinese Companies Are Not Purely Private, and Are Subject to Intrusive  
Laws Compelling Their Cooperation with Intelligence Agencies ..... 6

    C. ByteDance Is Subject to Significant CCP Influence..... 7

    D. TikTok’s U.S. Operations, Including Its Mass Collection of Data on U.S.  
Users ..... 8

III. The Government’s Response to these Growing Threats..... 10

    A. The President Issues Executive Order 13873 ..... 10

    B. The President Takes Action Relating to TikTok ..... 11

    C. The Department of Commerce’s Restrictions..... 12

Standard of Review..... 13

Discussion..... 14

I. Plaintiffs Have Not Established a Likelihood of Success on the Merits ..... 14

    A. The *Commerce Identification* Is Consistent with IEEPA and the Berman  
Amendment..... 14

        1. The Secretary Regulated Business-to-Business Transactions, Not  
Personal Communications ..... 15

        2. The Secretary Likewise Did Not Regulate Informational Materials ..... 17

    B. The Government’s Actions Are Consistent with the Administrative  
Procedures Act ..... 20

1.	Plaintiffs’ Arbitrary and Capricious Claims Are Not Reviewable .....	20
2.	The Secretary Acted Rationally in Identifying the Prohibited Transactions .....	22
3.	The Secretary’s Decision Was Not Pretextual .....	27
C.	The Government’s Actions Do Not Violate the First Amendment .....	29
1.	The Challenged Restrictions Are Not Subject to First Amendment Scrutiny Because They Are Directed at Business Transactions.....	29
2.	At Most, Some Form of Intermediate Scrutiny Would Apply, Which the Prohibitions Amply Satisfy .....	32
D.	The Challenged Actions Do Not Violate Procedural Due Process .....	36
E.	The President’s Actions Are Otherwise Consistent with IEEPA .....	37
II.	Plaintiffs Have Not Proven Immediate, Urgent Irreparable Harm Justifying a Preliminary Injunction .....	38
III.	The Balance of the Equities and Public Interest Strongly Favor the Government .....	43
IV.	Any Relief Should Be Appropriately Limited, and Require Posting of a Bond .....	44
	Conclusion .....	45

## INTRODUCTION

Federal government officials have long expressed concern about the Chinese government's ability to acquire Americans' private data through its control over Chinese companies that collect information from Americans. It is well-recognized that large Chinese technology firms are not purely private, but in fact are intertwined with and subject to the control and influence of the Chinese Communist Party ("CCP") and the government of the People's Republic of China ("PRC"). Moreover, Chinese law imposes broad obligations on citizens and companies to cooperate with the PRC by providing data and technological support to security and intelligence agencies and the military.

ByteDance Ltd. is a Chinese firm of particular concern for the U.S. Government. ByteDance is headquartered in Beijing, subject to PRC intelligence laws, and contains an internal corporate CCP committee through which the CCP exercises influence at the company. Moreover, its founder and CEO has publicly affirmed that ByteDance is a mouthpiece for the CCP in that it is committed to promoting the CCP's agenda and messaging. One of ByteDance's assets is the social media application TikTok, which collects vast quantities of data from its users including U.S. persons within the United States. When those users submit to TikTok's Terms of Service and Privacy Policy, they agree that their data may flow to ByteDance and (as such) may be turned over to the PRC. The President determined that the PRC's ability to control this data presented an unacceptable threat to the United States' national security and foreign policy. Accordingly, he exercised his authority under federal law to block certain business-to-business transactions involving ByteDance—action that would inhibit ByteDance's ability to collect Americans' data.

Plaintiffs challenge that determination by the President, as well as a subsequent action by the Secretary of Commerce ("Secretary") effectuating the President's determination. Plaintiffs seek emergency relief, requesting that this Court enter an order that would inject the Court into the

political Branches' handling of an ongoing threat posed by a foreign power and agents of that foreign power to national security and foreign policy interests of the United States.

The Court should reject Plaintiffs' request. As reflected in the twenty-five page decision memorandum attached to this filing, and other materials on which the Secretary relied, the Secretary made a reasoned, considered decision about the need to impose these prohibitions. That alone undercuts and rebuts Plaintiffs' likelihood of success on the merits, particularly in an area where the judgments of the President and the Secretary, both of whom are acting pursuant to clear statutory authority, are entitled to maximal judicial deference. Likelihood of success on the merits aside, Plaintiffs have also failed to carry their burden with respect to the other elements for a preliminary injunction. Plaintiffs have not proven any irreparable harm specifically flowing from the only set of prohibitions currently at issue, *i.e.* the prohibitions scheduled to go into effect on September 27 that would prevent new users from downloading TikTok, and would prevent existing users from automatically receiving updates of the application, but would otherwise allow TikTok's existing users to continue using the platform. Additionally, the public interest tilts decidedly *against* Plaintiffs insofar as their requested relief would necessarily infringe on the President's authority to block business-to-business economic transactions with a foreign entity in the midst of a declared national-security emergency, and their request for such intrusive relief should be denied.

## **BACKGROUND**

### **I. Statutory Framework**

#### **A. The International Emergency Economic Powers Act**

For nearly its entire history, the United States has used economic sanctions as a critical means to protect national security and achieve foreign policy goals. During most of the twentieth century, U.S. sanctions programs were governed by the Trading With the Enemy Act (TWEA), which granted the President "broad authority" to "investigate, regulate . . . prevent or prohibit . . .

transactions” in times of war or declared national emergencies. *See* 50 U.S.C. § 4305(b)(1); *see also Dames & Moore v. Regan*, 453 U.S. 654, 672 (1981).

In 1977, Congress enacted the International Emergency Economic Powers Act (IEEPA). *See* Pub. L. No. 95-223. IEEPA limited TWEA to periods of declared wars, but also provided the President with similar peacetime authority pursuant to declared national emergencies. *See Regan v. Wald*, 468 U.S. 222, 227-28 (1984). The broad powers granted to the President under IEEPA are essentially the same as those under TWEA, but IEEPA provides authority for the President to exercise those powers during peacetime, “to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat.” 50 U.S.C. § 1701(a). Once a national emergency relating to such a threat is declared, IEEPA empowers the President to:

[R]egulate, direct and compel, nullify, void, prevent or prohibit, any . . . transfer . . . of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest . . . with respect to any property, subject to the jurisdiction of the United States[.]

*Id.* § 1702(a)(1)(B).

### **B. The National Emergencies Act**

Congress enacted the National Emergencies Act (NEA), Pub. L. No. 94-412, 90 Stat. 1255 (1976) (codified as amended at 50 U.S.C. §§ 1601-1651), to “establish procedural guidelines for the handling of future emergencies with provision for regular Congressional review.” S. Rep. No. 94-922, at 1 (1976). The statute prescribes rules for Presidential declarations of national emergencies with respect to statutes “authorizing the exercise, during the period of a national emergency, of any special or extraordinary power.” 50 U.S.C. § 1621(a). Congress did not define the term “national emergency” or place any conditions on the President’s ability to declare a

national emergency. Instead, Congress committed this determination to the President as “it would be wrong to try to circumscribe with words with what conditions a President might be confronted.” *Nat’l Emergencies Act: Hr’gs Before the Subcomm. on Admin. Law and Governmental Relations*, 94th Cong. 27 (March 6, 1975) (statement of Sen. Mathias); *id.* at 27 (statement of Sen. Church).

Congress gave itself the exclusive oversight authority over a President’s national emergency declaration. For instance, declarations of national emergencies must “immediately be transmitted to the Congress,” 50 U.S.C. § 1621(a), and the President must comply with extensive congressional reporting requirements pertaining to that declaration, *id.* § 1641(a)-(c). Congress may terminate a national emergency through a joint resolution that is subject to fast track procedures, and Congress must meet “[n]ot later than six months after a national emergency is declared, and [every six months thereafter],” to consider whether the emergency shall be terminated. *Id.* § 1622(a)-(c).

## **II. Factual Background on the PRC, ByteDance, and TikTok**

Attached to this filing is the Secretary of Commerce’s decision memorandum setting forth the rationale for the Department of Commerce’s challenged actions. *See* 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) (“*Commerce Decision Memo*”), Ex. 1. The factual background set forth below is based on that memorandum and the underlying materials cited therein.<sup>1</sup>

---

<sup>1</sup> For clarity, the materials cited below and attached to this memorandum do not comprise the full administrative record. A complete, certified administrative record was not available for submission to the Court given the timeframe for this filing. The Government reserves the right to supplement the factual record at a later date, with the complete record and/or any other material the Government believes is appropriately considered in this action. *Cf.* Local Civil Rule 7(n)(1) (requiring an index of the administrative record “within 30 days following service of the answer to the complaint or simultaneously with the filing of a dispositive motion, whichever occurs first”).

**A. The PRC Is a Significant and Growing National Security Threat**

According to the United States Intelligence Community's Worldwide Threat Assessment for 2019, "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems." Daniel R. Coats, Director of National Intelligence ("DNI"), *Stmt. for the Record: Worldwide Threat Assessment of the U.S. Intelligence Cmty.* (2019) ("2019 Threat Assessment"), Ex. 2 at 5. In particular, the DNI stated that "China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies," and expressed concern "about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies." *Id.* Moreover, the Director of the FBI has stated that "[t]he greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China." *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, Speech at the Hudson Institute (July 7, 2020), Ex. 3 at 1.

One of the tools that the PRC uses to further its goals is bulk data collection. "The PRC Government has engaged in data collection on a massive scale across multiple domains as a means of generating information to enhance state security—and the political security of the CCP." *Commerce Decision Memo*, at 5. These large data sets "can reveal patterns and trends in human behavior, providing a 'pattern of life' that can be used to facilitate intelligence and surveillance targeting, particularly when aggregated with other data sets." *Id.* at 6. And the PRC is specifically "building massive databases of American's personal information," as part of a "tactic used by the Chinese government to further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment." *Id.*; *see also* Australian

Strategic Policy Institute (“ASPI”), *Engineering Global Consent: The Chinese Communist Party’s data-driven power expansion* (Oct. 2019), Ex. 4 at 3 (“By leveraging state-owned enterprises (SOEs), Chinese technology companies and partnerships with foreign partners . . . the CCP is building a massive and global data-collection ecosystem.”).

**B. Chinese Companies Are Not Purely Private, and Are Subject to Intrusive Laws Compelling Their Cooperation with Intelligence Agencies**

The PRC exercises “authority and supervision over nominally private or non-governmental organizations,” including through Party Committees or Corporate CCP Committees at those entities. *Commerce Decision Memo*, at 7. “Within private enterprises, the Party Committee implements CCP’s policies” and are a “source of political pressure across the boardroom.” *Id.*

Additionally, the PRC Government has enacted several laws increasing its influence “over all Chinese companies, and citizens[.]” *Commerce Decision Memo*, at 9. Notably, in 2017 the PRC enacted the National Intelligence Law, which “obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of intelligence work.” *Id.* at 10. The law expressly “permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation,” as well as “take control of an organization’s facilities, which includes communications equipment.” *Id.* at 10. Other PRC laws likewise require cooperation by company network operators. *See id.* Due to the lack of an independent judiciary in the PRC, there is no meaningful legal recourse for companies to challenge orders or requests from PRC intelligence or security agencies. *Id.*<sup>2</sup>

---

<sup>2</sup> Although not expressly noted in the *Commerce Decision Memo*, these same concerns have prompted Congress to legislate, including recently in the defense appropriations bill for FY2019. That law prohibited, *inter alia*, government agencies from buying or contracting with entities that use certain equipment or services produced by any “entity that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of [the PRC].” McCain National Defense Authorization Act, Pub. L. No. 115-232 § 889(f)(3)(D), 132 Stat. 1636, 1918 (2018). Congress also directed the President to assess and

### C. ByteDance Is Subject to Significant CCP Influence

TikTok’s parent company, ByteDance, Ltd., has its headquarters in Beijing and was founded in 2012 by entrepreneur Zhang Yiming. *See Commerce Decision Memo*, at 3. “ByteDance has significant and close ties to the CCP which could potentially be leveraged to further their agenda and exact pressure on ByteDance.” *Id.* at 7. In April 2018, the CCP forced ByteDance to shutdown one of its other platforms, and Mr. Yiming issued a public apology in which he pledged to cooperate with and elevate official CCP media. *See Foreign Policy, ByteDance Can’t Outrun Beijing’s Shadow* (Jan. 16, 2019), Ex. 5 at 2; China Media Project, *Tech Shame in the “New Era”* (Apr. 11, 2018), Ex. 6 at 5 (quoting Mr. Yiming’s apology as stating that “I am responsible because I failed to live up to the guidance and expectations supervisory organs have demanded all along,” and “[o]ver the past few years, the regulatory authorities have provided us with much guidance and assistance, but in our hearts we failed to properly understand and recognise [their demands]”); *see also Commerce Decision Memo*, at 8-9. Following this public atonement, ByteDance underwent organizational restructuring with CCP infrastructure now built into it. *Commerce Decision Memo*, at 8.

Since then, ByteDance has hosted several CCP-themed events at the company, *id.* at 8-9, and overall has demonstrated its commitment to CCP directives. *Id.* at 10-11. ByteDance has also signed an official cooperation agreement with a PRC security agency:

On April 25, 2019, ByteDance signed a strategic cooperation agreement with the Ministry of Public Security’s Press and Publicity Bureau in Beijing “aiming to give full play to the professional technology and platform advantages of Toutiao and Tiktok in big data analysis,” strengthen the creation and production of “public

---

formulate strategies to address the threat posed by China, including the CCP’s “use of political influence, information operations, censorship, and propaganda to undermine democratic institutions[,]” and the “use of economic tools, including market access and investment to gain access to sensitive United States industries.” *Id.* § 1261(b)(2)(A), § 1260(5). Congress also directed the Secretary of Commerce to provide detailed reporting “on foreign direct investment transactions made by entities of the [PRC] in the United States.” *Id.* § 1719(b)(1).

security new media works,” boost “network influence and online discourse power,” and enhance “public security propaganda, guidance, influence, and credibility,” among other aspects.

*Commerce Decision Memo*, at 11. Moreover, ByteDance appears to censor political content that is critical of China’s government or policies. *Id.* at 12-13.

**D. TikTok’s U.S. Operations, Including Its Mass Collection of Data on U.S. Users**

ByteDance owns the international social media application TikTok, which includes approximately 30 million monthly active U.S. users. *Commerce Decision Memo*, at 4. When a user signs up for a TikTok account, they agree to TikTok’s Terms of Service, including the Privacy Policy. *See* Exs. 7, 8. Under this Privacy Policy, TikTok collects a massive amount of user data, including:

1) registration information, such as age, username and password, language, and email or phone number; 2) profile information, such as name, social media account information, and profile image; 3) user-generated content, including comments, photographs, videos, and virtual item videos that you choose to upload or broadcast on the platform; 4) payment information, such as PayPal or other third-party payment information (where required for the purpose of payment); 5) phone and social network contacts (names and profiles); 6) opt-in choices and communication preferences; 7) information in correspondence users send to TikTok; and 8) information sent by users through surveys or participation in challenges, sweepstakes, or contests such as gender, age, likeness, and preferences.

*Commerce Decision Memo*, at 13. TikTok also “collects data on how the application including user behavior such as browsing and search history and technical and network details such as Internet protocol (IP) address, geolocation-related data, unique device identifiers, and cookies,” as well as “information from third parties, such as advertising and analytics partners.” *Id.* In other words, TikTok collects a tremendous amount of user data, “allow[ing] a very detailed picture of an individual user to be created,” *Commerce Decision Memo*, at 15, for example because TikTok automatically tracks and collects data on the location of every TikTok user in the United States.

TikTok’s Privacy Policy expressly states that TikTok “may share your information with a

parent, subsidiary, or other affiliate of our corporate group,” Ex. 8 at 6, which would allow TikTok to share user data with its parent company ByteDance. The Privacy Policy also states that it may disclose user data “to respond to . . . law enforcement requests, legal claims, or government inquiries.” *Id.* Regardless of these policies, “ByteDance is subject to PRC jurisdiction, [and] PRC laws can compel cooperation from ByteDance, regardless of whether ByteDance’s subsidiaries are located outside the territory of the PRC.” *Commerce Decision Memo*, at 19.

Despite being separate companies, TikTok’s infrastructure is not wholly separate from ByteDance. Some TikTok source code regarding “storage, internal management, and algorithms is still ‘partially shared across other ByteDance products.’” *Commerce Decision Memo* at 15. In its early years (pre-February 2019), TikTok stored its U.S. user data in China. *Id.* at 16. [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] *Commerce Decision Memo*, at 16. [REDACTED]

[REDACTED] is a Chinese company and, like ByteDance, is similarly beholden to PRC laws that require assistance in surveillance and intelligence operations.” *Id.* And despite claiming that data from U.S. users does not flow to China, a recent study “found that 37.70% of the IP addresses the TikTok Android package kit (APK) source code connects to are based in China,” [REDACTED]

[REDACTED]

Finally, TikTok also engages in censorship of politically sensitive content as to its U.S. users, particularly as to content inconsistent with the CCP’s views. *See Commerce Decision Memo*, at 12-13; *see also* ASPI, *TikTok and WeChat: Curating and Controlling Global Information*

*Flows*, Policy Brief, Report No. 37 (Sept. 2020), Ex. 9 at 4-24. As ASPI states, “[p]ossessing and deploying the capability to covertly control information flows, across geographical regions, topics and languages, positions TikTok as a powerful political actor with a global reach.” *Id.* at 2.

### **III. The Government’s Response to these Growing Threats**

#### **A. The President Issues Executive Order 13873**

On May 15, 2019, the President issued Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689, 22689 (the “ICTS Order”). The President explained “that the unrestricted acquisition or use in the United States of information and communications technology or services . . . supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.” *Id.*

In light of these findings, the President invoked his authority under the Constitution and the laws of the United States, including IEEPA and the NEA, to declare a national emergency with respect to this threat, and to prohibit certain transactions with foreign countries or foreign nationals that pose risks to the United States’ national security. *Id.* at 22690. On May 13, 2020, the President renewed the declaration of emergency set forth in the ICTS Order. *See* 85 Fed. Reg. 29321. Shortly thereafter, he presented a report to Congress, in accordance with the NDAA, outlining strategies in relation to the country’s foreign policy with China. *Id.*<sup>3</sup>

---

<sup>3</sup> Available at <https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf>.

**B. The President Takes Action Relating to TikTok**

On August 6, 2020, the President invoked the national emergency declared in the ICTS Order and determined that additional steps were necessary with respect to TikTok given its foreign ownership. *See* Exec. Order 13942, *Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*, 85 Fed. Reg. 48637 (Aug. 6, 2020) (“TikTok Order”). In particular, the President explained that TikTok “automatically captures vast swaths of information from its users, including internet and other network activity information such as location data and browsing and search histories.” *Id.*, pmbl.

The President assessed that this data collection poses several distinct risks. First, there is a risk the CCP will gain “access to Americans’ personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.” *Id.* In addition, the President highlighted concerns regarding TikTok’s “reported[] censors[ship] [of] content that the [CCP] deems politically sensitive,” *id.*, as well as concerns regarding the ways in which TikTok “may also be used for disinformation campaigns that benefit the [CCP], such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus.” *Id.* Finally, the President noted that other countries had taken action against TikTok. *Id.* The President concluded that it is time for the country to “take aggressive action against the owners of TikTok to protect our national security.” *Id.* Accordingly, the President provided that certain transactions with ByteDance or its subsidiaries would be prohibited and directed the Secretary of Commerce to identify the prohibited transactions within 45 days of the order. *Id.* § 1

In addition to the Executive Order challenged here, in August the President also ordered ByteDance to divest the U.S. operations and assets of TikTok, including all rights or interests

ByteDance may have in data obtained from U.S. users of TikTok. *See Order of August 14, 2020 Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297 (Aug. 14, 2020). Based on this action, there are ongoing, active discussions related to a possible corporate restructuring of TikTok and its U.S.-based activities, to provide greater ownership and control by U.S. businesses. *See, e.g., Georgia Wells and Aaron Tilley, Oracle Will Review TikTok Source Code to Watch for Chinese Access*, Wall Street Journal (Sept. 16, 2020).

### **C. The Department of Commerce's Restrictions**

Consistent with the President's Executive Order, on September 18, 2020, the Secretary of Commerce published a list of five transactions that will be prohibited with respect to ByteDance and its operations within the United States. On September 19, 2020, the Secretary revised the implementation date for one of the sets of prohibitions, and re-published the list of transactions:

1. Any provision of services, occurring on or after 11:59 p.m. eastern standard time on September 27, 2020, to distribute or maintain the TikTok mobile application, constituent code, or application updates through an online mobile application store[;]
2. Any provision of internet hosting services, occurring on or after 11:59 p.m. eastern standard time on November 12, 2020, enabling the functioning or optimization of the TikTok mobile application[;]
3. Any provision of content delivery network services, occurring on or after 11:59 p.m. eastern standard time on November 12, 2020, enabling the functioning or optimization of the TikTok mobile application[;]
4. Any provision of directly contracted or arranged internet transit or peering services, occurring on or after 11:59 p.m. eastern standard time on November 12, 2020, enabling the functioning or optimization of the TikTok mobile application[;]
5. Any utilization, occurring on or after 11:59 p.m. eastern standard time on November 12, 2020, of the TikTok mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the land and maritime borders of the United States and its territories[.]

*Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and*

*Communications Technology and Services Supply Chain* (Sept. 21, 2020) (“*Commerce Identification*”), see ECF No. 15-35.

As noted in the paragraphs, the Secretary identified phased implementation dates for the prohibited transactions. The Secretary determined that only “Transaction 1 should be prohibited immediately as it directly limits the availability of the app to new users for download and thus limits the growth of U.S. user data at risk.” *Commerce Decision Memo*, at 22. That set of prohibitions “would have the biggest impact in mitigating national security risks” while also “allowing the USG the latitude to further evaluate the viability of national security mitigations in the context of CFIUS [Committee on Foreign Investment in the United States] negotiations.” *Id.* Out of all the transactions, “transaction one allows for the greatest mitigation to national security while affecting the least number of parties and, in our estimation, being the easiest to implement,” and thus that set of transactions was prohibited earlier, whereas the implementation date for the other prohibitions was set at November 12, to align with the deadline for the President’s August 14 divestiture order. *See id.*

Importantly, the Secretary’s Identification also included several limitations. The Secretary expressly stated that “[t]he identified prohibitions herein only apply to the parties to business-to-business transactions[.]” *Commerce Identification* at 7. Similarly, “[t]hese identified prohibitions do not apply to . . . [t]he exchange between or among TikTok mobile application users of personal or business information using the TikTok mobile application[.]” *Id.* Additionally, the Secretary made clear that the prohibitions do not include any transactions related to the corporate restructuring of TikTok’s U.S. operations pursuant to the divestment order. *See id.* at 8.

#### **STANDARD OF REVIEW**

Plaintiffs here have moved for a preliminary injunction, which is “an extraordinary and drastic remedy[.]” *Munaf v. Geren*, 553 U.S. 674, 689 (2008). A party seeking such relief “must

establish that [it] is likely to succeed on the merits, that [it] is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [its] favor, and that [a temporary restraining order] is in the public interest.” *Winter v. NRDC*, 555 U.S. 7, 20 (2008). When “the Government is the opposing party,” the assessment of “harm to the opposing party” and “the public interest” merge. *Nken v. Holder*, 556 U.S. 418, 435 (2009). Injunctive relief that “deeply intrudes into the core concerns of the executive branch”—including foreign affairs and national security—may be awarded only upon “an extraordinarily strong showing” as to each element. *Adams v. Vance*, 570 F.2d 950, 954-55 (D.C. Cir. 1978).

## DISCUSSION

### I. Plaintiffs Have Not Established a Likelihood of Success on the Merits

#### A. The *Commerce Identification* Is Consistent with IEEPA and the Berman Amendment

Plaintiffs first claim that the *Commerce Identification* conflicts with the limited exceptions under IEEPA applicable to “personal communications” and, under the so-called Berman Amendment, to “information and informational materials.” *See* 50 U.S.C. § 1702(b)(1), (3). The text of those exceptions provide:

The authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly--

(1) any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value; . . .

(3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 4604 of this title, or under section 4605 of this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by chapter 37 of Title 18[.]

50 U.S.C. § 1702(b). Neither of these subsections precludes the Secretary’s actions here.<sup>4</sup>

**1. The Secretary Regulated Business-to-Business Transactions, Not Personal Communications**

With respect to subsection (b)(1), neither the President nor the Secretary of Commerce regulated “any personal communication, which does not involve a transfer of anything of value.” As set forth above, the Executive Order does not prohibit personal communications; it prohibits specific “*transactions . . . with ByteDance . . . or any subsidiary*” relating to TikTok and its U.S. operations. TikTok Order § 1(a) (emphasis added). The Secretary’s Identification likewise specifically excludes personal communications, and applies only to business-to-business transactions described in the Identification. *See Commerce Identification* at 7 (explaining that the prohibitions do not apply to the exchange “between or among TikTok mobile application users of personal or business information”). The prohibited transactions thus are not “personal communication[s]” within the meaning of the statute.

Plaintiffs describe the purpose of this prohibition as ensuring that IEEPA complies with the First Amendment. *See* Pls.’ Br. at 16. Such an understanding further undermines the claim that the Secretary’s actions here run afoul of § 1702(b)(1), because there is no plausible First Amendment right to engage in business-to-business transactions with respect to things like Internet hosting services or Internet peering services with a foreign entity that poses a national-security threat to the United States. *See Commerce Identification*, ¶¶ (2), (4). If TikTok is concerned about the underlying communications on its platform being impacted, it is free to restructure its business

---

<sup>4</sup> Plaintiffs have submitted what appears to be an attempt at an expert witness declaration from Professor Amanda Tyler addressing the history of IEEPA and these provisions. *See* ECF No. 15-5. This declaration opines on legal conclusions, not factual matters for which expert testimony is appropriate, and the Court should therefore disregard the declaration. *Cf. Burkhardt v. Washington Metro. Area Transit Authority*, 112 F.3d 1207, 1212–13 (D.C.Cir.1997) (“[A]n expert may offer his opinion as to facts, that, if found, would support a conclusion that the legal standard at issue was satisfied, but he may not testify as to whether the legal standard has been satisfied”).

operations to eliminate the national-security threat identified under IEEPA and ensure that those communications can continue.

Nor can the “personal communications” exception be invoked by relying on TikTok content itself, as opposed to the transactions that have been prohibited, because content provided via TikTok plainly involves “a transfer of anything of value,” in at least three respects. First, according to Plaintiffs’ own theory of this case, a user’s mere presence on (and use of) the TikTok platform is a principal and essential source of value for TikTok as a company. *See, e.g.*, Tr. of Sept. 24 Status Conf. at 13 (Plaintiffs’ counsel asserting that “we know in the social media business, new users, retaining users, is absolutely the lifeblood of the business”).

Second, when users sign up for TikTok, they agree to exchange their sensitive personal data for the right to use TikTok services. *See* TikTok Terms Of Service, Ex. 7 at 2. Additionally, when users exchange communications on TikTok, in doing so they are granting TikTok “an unconditional irrevocable, non-exclusive, royalty-free, fully transferable, perpetual worldwide licence to use . . . publish and/or transmit, and/or distribute and to authorise other users of the Services and other third-parties to view, access, use . . . your User Content in any format and on any platform.” *Id.* at 8; *see also id.* at 6 (“You acknowledge and agree that we may generate revenues, increase goodwill or otherwise increase our value from your use of the Services”). Accordingly, user activity on TikTok plainly involves an exchange of value from the user to TikTok.

Third, content created and provided on TikTok also provides value to its user-creators. Indeed, a group of TikTok content creators recently challenged the Executive Order and the Secretary’s Identification relating to TikTok in a separate action in the Eastern District of Pennsylvania. *See Marland et al. v. Trump et al.*, ECF No. 7, 20-cv-4597 (E.D. Pa., September

19, 2020). While these plaintiffs likewise do not identify a valid basis on which to enjoin the challenged actions, their claims do demonstrate that TikTok creators are able to earn money, or even make a “career creating and posting content,” purporting to make thousands of dollars month from their activities both on TikTok and from related “brand and sponsorship deals.” *Id.* at 5, 18; *see also* Pappas Decl. (ECF No. 15-3) ¶ 22. For this reason as well, content provided via TikTok clearly involves value and thus the exemption in § 1702(b)(1) is irrelevant.

## 2. The Secretary Likewise Did Not Regulate Informational Materials

Section 1702(b)(3) is also inapposite. That provision excepts from the President’s authority under IEEPA the power to regulate or prohibit the importation or exportation of information or informational materials to or from a country. But again, the *Commerce Identification* does not prohibit any importing or exporting of information (tangible or intangible)—the Identification simply prohibits business-to-business economic transactions that support certain aspects of TikTok’s U.S. operations.

Even assuming that the content that users choose to post on TikTok could be construed as “information” or “informational materials,” the *Commerce Identification* does not say or do anything to TikTok users themselves. Again, the *Commerce Identification* expressly carves out users’ ability to continue communication. Moreover, TikTok itself does not constitute “information” or “information materials”; rather, it is a set of services through which information of that type may be conveyed. *See generally* TikTok Terms of Service, Ex. 7 at 1 (repeatedly referring to the app as a suite of “services”). TikTok is, by its own terms, a diverse set of services, that (among other things) manipulates, collects, processes, transmits, brokers, and sells information, *see id.* at 2-6, thus bearing no resemblance to the examples of exempted media listed in the statutory text—*i.e.*, “publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.”

The regulation of a single service provider is not akin to regulating or prohibiting transmission of information or informational materials themselves, nor to an indirect restriction on them through limitations imposed on an entire “medium of transmission.” Any construction that would collapse that distinction between restricting the flow of information writ large, and restricting a single service provider (with ties to a foreign adversary), would amount to a wholesale truncation of the President’s ability to protect the country’s information supply chains in a way that Congress could not have intended. For example, it is unfathomable that Congress intended through section 1702(b) to limit the President’s ability to prevent a foreign government—including, under TWEA, a wartime enemy—from setting up a parallel postal system in the United States or dominating the country’s data services. Yet that absurd conclusion would necessarily flow from interpreting subsection (b)(3) in the way Plaintiffs suggest. There is no indication that Congress intended that outcome. *See King v. Burwell*, 576 U.S. 473, 494 (2015) (rejecting interpretation because it was “implausible that Congress meant the Act to operate in this manner”).

Congress did not intend to preclude the President from invoking IEEPA to regulate particular entities simply because those entities happen to engage in transmitting information themselves, or because they facilitate others’ transmission of information. Indeed, Congress has specifically made clear that IEEPA can be used to “block and prohibit *all* transactions in *all* property and interests” of persons and entities who “engage[] in, support[], facilitate[], or benefit[] from the significant appropriation, through economic or industrial espionage *in cyberspace*, of technologies or proprietary information developed by United States persons.” 50 U.S.C. § 1708(b)(1), (2) (emphases added). If § 1702(b)(3) were as broad as Plaintiffs suggest, the authority granted in § 1708 would be of little effect: even if the President identified a person engaging in economic espionage in cyberspace, for example the President could not prohibit

transactions in that person's computer because that computer is a means by which information and informational materials is transmitted. There is neither a statutory basis for this cramped interpretation, nor a basis in First Amendment law. *See* Part I.C, *infra*.

Indeed, the Office of Foreign Assets Control ("OFAC") has promulgated regulations specifically interpreting these provisions of IEEPA, *see* 31 C.F.R. § 501, *et seq.*, and Plaintiffs themselves rely on these regulations as representative of "the executive branch's historical practice of implementing its IEEPA authority." Pls.' Br. at 19. And here, the regulations make clear that the "informational materials" exemption does not include "materials not fully created and in existence at the date of the transactions." 31 C.F.R. § 560.210(c)(2). In other words, materials not fully created as of the date of a transaction can still be prohibited, because they fall outside § 1702(b)(3).

Here, even if Plaintiffs' theory were correct that prohibiting economic transactions with TikTok should be analyzed the same as if it were prohibiting the transmission of the underlying materials on TikTok, *see* Pls.' Br. at 18-19, that still would not advance their claim because users interact with the TikTok application to create the content they will share on it and thus the underlying materials posted on TikTok are "not fully created and in existence" prior to users' interactions with TikTok. Notably, OFAC's regulation interpreting IEEPA in this manner was expressly upheld by the Third Circuit, *United States v. Amirmazmi*, 645 F.3d 564, 586 (3d Cir. 2011). That opinion catalogued in detail the "ample evidence to suggest Congress has accepted OFAC's decision to permit the circulation of informational materials already in existence while concomitantly regulating transactions that contemplate the creation of new materials." *Id.* at 587. As confirmed by OFAC's regulations and historical practice, therefore, TikTok content is outside the scope of § 1702(b)(3).

Finally, even if the TikTok application otherwise fell within § 1702(b)(3), it would nonetheless be excluded from that provision by the second sentence of that paragraph, which excepts from the exception “acts . . . prohibited by chapter 37 of Title 18.” Chapter 37 of Title 18, in turn, prohibits transmission of “information relating to the national defense” to any foreign government with reason to believe that it could “be used to the injury of the United States or to the advantage of a foreign nation.” 18 U.S.C. § 794; *see also id.* §§ 793(e), (f) (prohibiting similar activities, whether willful or grossly negligent in violation of a duty of trust). Because the TikTok Order takes action to prevent exactly such harms, and contemplates that the vast swaths of user information collected by TikTok is information relating to the national defense, it falls outside any limitations otherwise posed by § 1702(b)(3). Despite the downstream, incidental effects on TikTok users, *see* Part I.C.1, *infra*, the Secretary’s prohibitions are fully consistent with IEEPA.

**B. The Government’s Actions Are Consistent with the Administrative Procedures Act**

**1. Plaintiffs’ Arbitrary and Capricious Claims Are Not Reviewable**

Plaintiffs seek to challenge the *Commerce Identification* as arbitrary and capricious, but they overlook a threshold inquiry whether such claims are even reviewable. Under the terms of the TikTok Order, the Secretary of Commerce was instructed to identify prohibited transactions pursuant to the President’s IEEPA powers. *See* TikTok Order § 4. In effect, then, Plaintiffs are arguing that the Secretary acted arbitrarily in implementing IEEPA. But IEEPA does not permit Plaintiffs to invoke the APA to bring arbitrary and capricious claims.

**a.** The APA applies to agency actions “except to the extent that (1) statutes preclude judicial review; or (2) agency action is committed to agency discretion by law.” 5 U.S.C. § 701. On the first exception, “[w]hether and to what extent a particular statute precludes judicial review is determined not only from its express language, but also from the structure of the statutory scheme,

its objectives, its legislative history, and the nature of the administrative action involved.” *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 345 (1984). And the second exception applies when “the statute is drawn so that a court would have no meaningful standard against which to judge the agency’s exercise of discretion.” *Heckler v. Chaney*, 470 U.S. 821, 830 (1985).

Here, the NEA and IEEPA confer highly discretionary authority upon the President to act quickly and decisively to address threats to the United States, and the statutory structure suggests that Congress assigned itself sole oversight authority of the Executive’s actions. *See* Background, § I *supra*. The lack of APA reviewability is buttressed by the constitutional context in which Congress legislated. “National-security policy is the prerogative of the Congress and President.” *Ziglar v. Abbasi*, 137 S. Ct. 1843, 1861 (2017). Nothing in the NEA or IEEPA suggests an intent by Congress to invert the constitutional order by permitting an injunction of an Executive Order that addresses a national security threat, based solely on a third party’s complaints, particularly where Congress itself has not exercised its authority to terminate the relevant declaration, *see* 50 U.S.C. § 1622(a)(1). In fact, the text of IEEPA demonstrates just the opposite, making clear that a provision permitting judicial access to classified materials “does not confer or imply any right to judicial review.” 50 U.S.C. § 1702(c).

Moreover, when the President delegates authority to an agency to determine which transactions to prohibit under IEEPA, there are no manageable standards by which a court could evaluate the agency’s exercise of discretion. *Cf. People’s Mojahedin Org. of Iran v. Dep’t of State*, 327 F.3d 1238, 1244 (D.C. Cir. 2003) (holding that the question whether activity is “terrorist activity” that “threaten[s] the security of the United States or its nationals” is nonjusticiable, because “it is beyond the judicial function for a court to review foreign policy decisions of the Executive Branch”); *California v. Trump*, 407 F. Supp. 3d 869, 891 (N.D. Cal. 2019) (holding that

“whether the national emergency truly exists” is a “nonjusticiable political question[.]”). Because there are no meaningful standards by which this Court could evaluate the agency’s identification of prohibited transactions under IEEPA, the APA does not apply.<sup>5</sup>

**b.** At a minimum, this Court should not permit Plaintiffs to use the APA as a basis for a back-door challenge to the President’s Executive Order itself. It is well-established that the APA cannot be used to challenge an action of the President. *Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992). And even outside the context of the APA, “longstanding authority holds that [judicial] review is not available when the statute in question commits the decision to the discretion of the President.” *Dalton v. Specter*, 511 U.S. 462, 474 (1994).

Here, the President exercised his discretion, vested in him by the NEA and IEEPA, and determined that “action must be taken to address the threat posed by . . . TikTok,” and identified several concrete risks associated with the application. *See* TikTok Order, pmb1. The fact that the President then delegated authority to the Secretary of Commerce to determine how best to address those risks under IEEPA should not bring the President’s antecedent factual findings within the realm of judicial review. *See* Pls.’ Br. at 21. Even if the APA can be used to examine the Secretary’s decisions, it should not be used as a mechanism for a back-door challenge to the President’s factfinding and exercise of discretion.

## **2. The Secretary Acted Rationally in Identifying the Prohibited Transactions**

Plaintiffs argue that the Secretary “ignored the evidence before [him]” and “failed to

---

<sup>5</sup> In this respect, this case is different from other IEEPA designation cases, where the President has set forth clear standards in the Executive Order itself, and then this Court reviews whether the agency properly found that a particular individual or entity fit within those standards. *See, e.g., Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003). Here, the President’s Executive Order did not set forth any judicially manageable standards by which the Court could review the agency’s exercise of discretion.

consider reasonable alternatives,” Pls.’ Br. at 20, despite Plaintiffs not yet having seen the administrative record or even the Secretary’s decision memorandum. The *Commerce Decision Memo*, and the additional information cited therein, makes clear that the Secretary acted rationally in responding to the factual information before him.

a. The *Commerce Decision Memo* is a thorough, twenty-five page document that walks through the threats posed by the PRC and ByteDance, *see id.* at 5-13; why the United States is vulnerable to those threats, particularly with respect to ByteDance and Tiktok, *see id.* at 13-19; the consequences of those threats and vulnerabilities, *see id.* at 19-21; and recommendations for mitigating such threats, *see id.* at 22-24.

The *Commerce Decision Memo* specifically considers the evidence that ByteDance and TikTok submitted in response to the administrative subpoena. For example, although TikTok claimed to store U.S. user data within the United States, the *Commerce Decision Memo* then explained why the PRC may still be able to gain access to that data through [REDACTED]

[REDACTED] *See Commerce Decision Memo*, at 15-18. Moreover, even though TikTok insists that the Chinese government does not have access to U.S. user data, the Secretary found that “ByteDance cannot account for surveillance that may be conducted on its operations without its explicit knowledge or awareness at a corporate level.” *Id.* at 20. Indeed, there is reason for suspicion given the close ties generally between ByteDance and the CCP, *see id.* at 19-20, as well as the high level of activity between U.S.-based TikTok users and IP addresses located in China and owned by a Chinese company, *see id.* at 16. This network activity suggests that “some data from the TikTok app may be directly transmitted to China, bypassing ByteDance’s leased or owned servers altogether,” *id.*

at 16, which would make such data even easier for the PRC to access, *see id.* at 20 (discussing the numerous ways the PRC could gain access to ByteDance information, even without ByteDance’s knowledge).

Aside from the potential exposure of U.S. users’ data, the Secretary also found that TikTok could be exploited for censorship or propaganda for U.S.-based users, thereby affecting public opinion within the United States and urging it to align to the CCP’s preferred views. *See Commerce Decision Memo*, at 20-21. This risk is not hypothetical; it is active and ongoing, including on some of the most sensitive issues of today. *See id.* at 20-21 & n.157; *see also* Ex. 9 at 4-24.

**b.** Plaintiffs’ challenges to the Secretary’s actions are meritless. Plaintiffs first argue that “the government does not have *any* evidence that the Chinese government has ever obtained *any* TikTok U.S. user data.” Pls.’ Br. at 21. Even if that were accurate, IEEPA authorizes the President to regulate “*threat[s]*” that arise from “a source in whole or substantial part outside the United States.” 50 U.S.C. § 1701(a) (emphasis added). The statute vests the President with discretion to determine whether, when, and how best to respond, stating that the President “*may*” exercise his authorities in such circumstances, *id.* (emphasis added). There is no requirement that the Executive must wait for specific harm to occur before responding—the Executive is free to act prospectively based on a risk of harm. *Cf. Trump v. Hawaii*, 138 S. Ct. 2392, 2421 (2018) (“[W]e cannot substitute our own assessment for the Executive’s predictive judgments on such matters, all of which are delicate, complex, and involve large elements of prophecy.”).

Plaintiffs also seek to submit several declarations, purportedly demonstrating that there is no risk of the PRC gaining access to U.S. user data. In APA cases, however, “the focal point for judicial review should be the administrative record already in existence, not some new record made

initially in the reviewing court.” *Camp v. Pitts*, 411 U.S. 138, 142 (1973). Thus, the submitted declarations are irrelevant and should be wholly disregarded.<sup>6</sup>

Even if the Court considered the declarations, they do not undermine the Secretary’s actions, and in fact only confirm that the risks do exist. For example, Mr. Cloutier’s declaration—from an individual who has been with the company less than six months—touts that TikTok user data is stored in U.S. and Singapore data centers, *see* ECF No. 15-2 ¶ 8, but fails to acknowledge [REDACTED], as discussed above. Moreover, Mr. Cloutier confirms that “TikTok relies on China-based ByteDance personnel for certain engineering functions that require them to access encrypted TikTok user data,” and that these same personnel may receive decrypted data as well. *Id.* ¶ 10. Under China’s broad national intelligence and surveillance laws, these engineers (as Chinese citizens) could be compelled to share this user information with the PRC Government, which is a risk in and of itself. Finally, Mr. Cloutier refers to a “process of implementing additional protections to safeguard user data,” *id.* ¶ 11, but that new process only highlights the existing dangers in TikTok’s data storage, and Mr. Cloutier notably omits any detail about when these new initiatives began and when they are expected to be completed.

As for Ms. Pappas’s declaration, she touts the purported independence of the U.S. content-

---

<sup>6</sup> At a minimum, the Court should disregard the Weber declaration (ECF No. 15-4), which appears to be an attempt at expert witness testimony, but the declaration fails to meaningfully describe “the facts or data considered by the witness in forming” his opinions. Fed. R. Civ. P. 26(a)(2)(B)(ii). The declaration states that “I have reviewed the declaration of Roland Cloutier, TikTok’s Chief Security Officer, and have also reviewed other data security-related materials the company has made public,” ECF No. 15-4 ¶ 10, but does not specify what those other materials are, and thus the Government has no way of meaningfully evaluating the declaration. Moreover, it is rather curious that Plaintiffs hired a purported cybersecurity expert “to analyze the stated justifications of President Trump’s Executive Order . . . relating to the TikTok software application, *id.* ¶ 3, but then affirmatively chose *not* to provide that individual with access to any non-public material.

moderation team, and states that “[t]o my knowledge, there has never been a request from the Chinese government to moderate content on TikTok, and we would reject such a request for content moderation if we received one.” ECF No. 15-3 ¶ 15. But she does not explain if or how she would become aware of such a request, nor does she explain how TikTok and ByteDance could successfully resist such a request, given the Chinese laws that would compel such cooperation and offer no meaningful judicial recourse. *See Commerce Decision Memo*, at 10. In addition, there are numerous documented instances of censorship and content moderation on TikTok consistent with the preferred views of the CCP. *See Commerce Decision Memo*, at 12-13, 20-21; Ex. 9 at 4 (noting TikTok’s claimed independence, but stating that “the censorship techniques outlined below disprove some of those claims and, instead, suggest a preference for protecting and entrenching the sensitivities, and even prejudices, of some governments”). Ms. Pappas makes no effort to explain the ongoing censorship of political content, and the fact that it occurs without even being requested by the PRC Government only underscores the dangers associated with ByteDance and its closeness to the CCP.

c. Plaintiffs also argue that the Secretary failed to consider obvious alternatives. *See Pls.’ Br.* at 21-22. As noted above, however, the Secretary explained that, because ByteDance is a Chinese company closely aligned with the CCP, it is impossible for less restrictive alternatives to achieve the same national security ends. *See Commerce Decision Memo*, at 22.

Plaintiffs contend that the Government should have considered “the range of tools available pursuant to the CFIUS process[.]” *Pls.’ Br.* at 22. That argument might make sense if the agency action being challenged were a CFIUS decision; but the action at issue here is the Secretary’s Identification of Prohibited Transactions under IEEPA. It is far from clear why the Secretary was obligated to consider CFIUS alternatives when regulating under IEEPA; CFIUS is an entirely

separate administrative process, involving different legal authorities, and involves numerous decisionmakers beyond just the Secretary of Commerce.

In any event, Plaintiffs' argument is inconsistent with the record here. The *Commerce Decision Memo* makes clear that the Secretary was neither accepting nor rejecting any of the CFIUS alternatives; instead, he was acting to achieve the "biggest impact in mitigating national security risks" while also "allowing the USG the latitude to further evaluate the viability of national security mitigations in the context of CFIUS negotiations." *Commerce Decision Memo*, at 22. Thus, the Secretary did not "abandon" or "reject" those alternatives, Pls.' Br. at 22, but simply prioritized the immediate protection of national security while allowing more time for the CFIUS process to play out. There is nothing irrational about such an approach.<sup>7</sup>

### **3. The Secretary's Decision Was Not Pretextual**

As noted above, the Secretary's decision was thorough, reasoned, and well-explained in a lengthy decision memorandum. Plaintiffs assert, however, that the reasons proffered by the Secretary were pretextual and his actions should be invalidated on that basis. Pls.' Br. at 24-27.

As an initial matter, Plaintiffs' argument largely depends on their factual assertion that there are no valid national security risks associated with TikTok. *See id.* at 23-24. Because the factual record here confirms the Executive Branch's assessment that there are genuine national security risks—a conclusion to which this Court owes, at a minimum, significant deference—that record should itself be sufficient to defeat this argument. *See Dep't of Commerce v. New York*, 139 S. Ct. 2551, 2573 (2019) ("[A] court may not reject an agency's stated reasons for acting simply because

---

<sup>7</sup> Plaintiffs' argument also fails on its own terms. Plaintiffs describe a list of "wide-ranging and robust" mitigation measures that they claim to have offered, Pls.' Br. at 22, yet the document cited by Plaintiffs (Exhibit 22) fails to support any of those assertions. Plaintiffs have thus failed to substantiate their argument, and of course should not be permitted to submit new factual material as part of their reply.

the agency might also have had other unstated reasons.”).

Regardless, Plaintiffs’ argument is also wrong legally. As noted above, the only action that is (and could be) challenged in this APA claim is the Secretary of Commerce’s prohibitions. But Plaintiffs’ argument is based entirely on statements of *others*, not the Secretary of Commerce. Thus, it does nothing to undermine the actual decision that is before the Court. *See Ramos v. Wolf*, --- F.3d ----, 2020 WL 5509753, at \*19 (9th Cir. Sept. 14, 2020) (rejecting similar claim when there is no evidence that alleged animus “played any role in the [agency] decision-making process”). Moreover, the Secretary’s decision is supported by the presumption of regularity, and Plaintiffs bear the burden of rebutting that presumption. *See United States v. Chem. Found.*, 272 U.S. 1, 14-15 (1926) (“The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.”); *Hercules, Inc. v. EPA*, 598 F.2d 91, 123 (D.C. Cir. 1978) (explaining that “[e]xcept in cases where there is no accompanying explanation of the reasons underlying an [agency’s] decision, . . . [a] strong presumption of regularity supports the inference that when administrative officials purport to decide weighty issues within their domain they have conscientiously considered the issues,” and “[t]his presumption can be overcome, and further explication can be required of the decisionmaker, only upon a strong showing of bad faith or improper behavior.”). Finally, even taking Plaintiffs’ argument at face value, it hardly demonstrates impropriety for the President to be operating in the sphere of “public relations” while the Secretary is independently making his decision based on the record before him. *Dep’t of Commerce*, 139 S. Ct. at 2573 (“Agency policymaking is not a rarified technocratic process, unaffected by political considerations or the presence of Presidential power.”). Thus, the Secretary’s actions are fully consistent with the APA.

**C. The Government’s Actions Do Not Violate the First Amendment**

**1. The Challenged Restrictions Are Not Subject to First Amendment Scrutiny Because They Are Directed at Business Transactions**

All of Plaintiffs’ First Amendment arguments overlook a threshold point—whether the challenged restrictions are subject to First Amendment scrutiny in the first place. Consistent with IEEPA’s grant of authority to the President to regulate economic transactions, *see* 50 U.S.C. § 1702(a)(1)(B), both the Executive Order and the *Commerce Identification* prohibit only certain business transactions—not protected First Amendment activity.

Plaintiffs here do not claim a First Amendment right to engage in any of the regulated economic transactions themselves—*e.g.*, a right to “distribute or maintain the TikTok mobile application, constituent code, or application updates through an online mobile application store,” or a right to provide “internet hosting services . . . enabling the functioning or optimization of the TikTok mobile application.” *Commerce Identification*, ¶ (1). Presumably that is because economic regulations of this nature generally are not subject to First Amendment scrutiny, *see, e.g., Glickman v. Wileman Bros. & Elliott, Inc.*, 521 U.S. 457, 469-70 (1997), and because it is an “across-the-board restriction” on action “justified by weighty concerns of foreign policy.” *Regan v. Wald*, 468 U.S. 222, 241-42 (1984). Plaintiffs also do not claim a First Amendment right in hosting TikTok itself as a platform for others’ speech. Presumably that is because merely hosting a platform is not itself an exercise of the First Amendment. *See U.S. Telecom Ass’n v. FCC*, 825 F.3d 674, 741 (D.C. Cir. 2016) (“The absence of any First Amendment concern in the context of common carriers rests on the understanding that such entities . . . merely facilitate the transmission of the speech of others rather than engage in speech in their own right.”).

Instead, Plaintiffs rely on two alternate theories of how the First Amendment is implicated: (1) Plaintiffs themselves are speakers on TikTok; and (2) in TikTok’s source code. *See* Pls.’ Br.

at 27-28. Neither interest implicates the First Amendment here.

a. With respect to Plaintiffs themselves claiming to be speakers on TikTok, that interest effectively places them in the exact same position as every other user or speaker on TikTok. But users or speakers on TikTok cannot challenge the prohibited transactions because those prohibitions do not regulate expressive activity on TikTok.

Plaintiffs can argue, at most, that the Secretary's prohibited economic transactions will have a downstream effect on their ability to engage in expressive activity on TikTok itself. But such downstream, incidental effects on expressive activity generally do not justify First Amendment scrutiny of the challenged regulation. For example, in *Arcara v. Cloud Books, Inc.*, 478 U.S. 697 (1986), a bookstore ordered to be closed as a public nuisance sought to argue that “the effect of the statutory closure remedy impermissibly burdens its First Amendment protected bookselling activities,” but the Supreme Court rejected that argument because “every civil and criminal remedy imposes some conceivable burden on First Amendment protected activities,” and booksellers may not assert “First Amendment coverage to defeat a valid statute aimed at penalizing and terminating illegal uses of premises.” *Id.* at 705-707; *see also Virginia v. Hicks*, 539 U.S. 113, 123 (2003) (upholding a state trespass policy even as to those who trespass for First Amendment purposes, because “it is Hicks’ nonexpressive *conduct*—his entry in violation of the notice-barmen rule—not his speech, for which he is punished as a trespasser”); *Cohen v. Cowles Media Co.*, 501 U.S. 663, 669 (1991).

Here, the Executive Order and *Commerce Identification* prohibit business-to-business economic transactions with a foreign entity and its subsidiaries that pose a national-security threat to the United States, as determined by the President. The fact that those prohibitions may have adverse, downstream effects on a purported forum for Plaintiffs’ speech is legally irrelevant:

“Neither the basis for the . . . sanction . . . nor its purpose . . . has anything to do with the First Amendment.” *Hicks*, 539 U.S. at 123. Indeed, this point is proven by the fact that TikTok could continue its claimed expressive activity if it re-arranged its corporate structure to eliminate the national-security risks to the United States. Thus, the First Amendment is inapplicable to the Government’s challenged actions.<sup>8</sup>

**b.** As for Plaintiffs’ claimed First Amendment interest in their source code, they do not establish that their code “possesses sufficient communicative elements to bring the First Amendment into play.” *Texas v. Johnson*, 491 U.S. 397, 404 (1989). To be sure, some courts have held that source code can constitute protected speech when it is actually intended to communicate a message to someone. For example, in *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), the plaintiff was a professor who sought to distribute encryption source code to others, in order to help demonstrate how computers work. *Id.* at 483.

Here, however, Plaintiffs affirmatively do *not* want to communicate their underlying source code to anyone, and in fact have allegedly taken numerous steps to restrict and lock-down that source code. *See* Cloutier Decl. (ECF No. 15-2) ¶ 14 (“To maintain the integrity of our source code in light of our global workforce, we have dedicated workflow systems to make sure that employees must demonstrate a need for information before they can access source code.”). When the underlying computer code is not even being distributed to others, it does not constitute First Amendment protected activity, because there is simply no expressive activity involved. *See U.S.*

---

<sup>8</sup> Nor can Plaintiffs argue that TikTok has been singled out for special treatment, *cf. Arcara*, 478 U.S. at 704-05, because the prohibition of transactions pertaining to ByteDance is expressly part of the Government’s broader efforts to respond to the growing threats posed by China and its technology companies. *See* ICTS Order § I; Background § II, *supra*. Moreover, the Secretary’s simultaneous actions with respect to Tencent/WeChat, which pose analogous threats, do not reflect a phased approach, resulting in an allegation by WeChat users that the Government is actually advantaging TikTok. *See WeChat Users Alliance v. Trump*, No. 20-cv-5910 (N.D. Cal.).

*Telecom Ass’n*, 825 F.3d at 741 (“The Supreme Court has explained that the First Amendment comes ‘into play’ only where particular conduct possesses sufficient communicative elements, that is, when an intent to convey a particularized message is present, and in the surrounding circumstances the likelihood is great that the message would be understood by those who viewed it.” (modifications and citations omitted)); *see also, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 448 & n.20 (2d Cir. 2001) (upholding First Amendment protection for computer code when it “convey[s] information capable of comprehension and assessment by a human being” but not when “a human’s mental faculties do not intercede in executing the instructions”); *CDK Glob. LLC v. Brnovich*, --- F. Supp. 3d ----, 2020 WL 2559913, at \*12 (D. Ariz. May 20, 2020) (holding that there is no First Amendment interest when code “only tells a computer how to function; it has no other expressive purpose”).

**2. At Most, Some Form of Intermediate Scrutiny Would Apply, Which the Prohibitions Amply Satisfy**

Even if the Court concluded that the economic prohibitions implicate sufficient expressive activity to warrant First Amendment scrutiny, the prohibitions would be analyzed, at most, under some form of intermediate scrutiny. This standard is appropriate for analyzing a regulation of conduct that incidentally burdens speech, *see United States v. O’Brien*, 391 U.S. 367, 376 (1968), as well as “time, place, or manner” restrictions. *See United States v. Albertini*, 472 U.S. 675, 687-88 (1985) (applying the *O’Brien* standard to “[a]pplication of a facially neutral regulation that incidentally burdens speech”); *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 298 (1984) (equating the *O’Brien* standard to the standard for “time, place, or manner” restrictions); *see also Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of New York*, 447 U.S. 557, 563-64 (1980) (describing a similar standard for commercial speech restrictions).

Plaintiffs dispute that intermediate scrutiny would apply, and instead argue for strict

scrutiny, equating the prohibitions here to a prior restraint. Pls.’ Br. at 28. But “prior restraint” is a term of art in the First Amendment context, and neither of the Government’s actions here qualifies as such. A prior restraint is “used to describe administrative and judicial orders *forbidding* certain communications when issued in advance of the time that such communications are to occur.” *Alexander v. United States*, 509 U.S. 544, 550 (1993). Here, there is no direct, advance prohibition on any communications. Plaintiffs are not prohibited from doing or saying anything. Restrictions on economic transactions, even when involving a particular platform for communication, simply are not “prior restraints” within the meaning of First Amendment doctrine.

Under the intermediate scrutiny standard for evaluating time, place, or manner restrictions, Government restrictions on speech “are valid provided that they are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information.” *Clark*, 468 U.S. at 293. The Secretary’s prohibitions—and particularly the first paragraph, which is the only paragraph presently at issue—amply satisfy this standard.

First, the *Commerce Identification* is content-neutral, because it does not depend in any way on the content of the message being communicated. *See Reed v. Town of Gilbert*, 576 U.S. 155, 166 (2015) (setting forth the relevant test). Plaintiffs do not appear to contend otherwise. *See* Pls.’ Br. at 29.

Second, the restrictions are narrowly tailored to serve a significant governmental interest. The “sensitive and weighty interests of national security and foreign affairs” are critically important Government interests. *Holder v. Humanitarian Law Project*, 561 U.S. 1, 33-34 (2010); *see also Haig v. Agee*, 453 U.S. 280, 307 (1981). And in the First Amendment context, narrow tailoring is satisfied “so long as the neutral regulation promotes a substantial government interest

that would be achieved less effectively absent the regulation.” *Albertini*, 472 U.S. at 689; *see also Clark*, 468 U.S. at 297 (“[I]f the parks would be more exposed to harm without the sleeping prohibition than with it, the ban is safe from invalidation under the First Amendment[.]”).

Pursuant to the President’s findings, “TikTok automatically captures vast swaths of information from its users, including internet and other network activity information such as location data and browsing and search histories.” TikTok Order, pmbl. Because this danger is inherent in the application itself, the Government sensibly responded first by prohibiting new users within the United States from downloading the application (and then ultimately prohibiting transactions that enable the U.S. operations of the application). The United States’ national security and foreign affairs interests would obviously be achieved less effectively absent these restrictions, *i.e.*, if TikTok were allowed to continue operating in an unrestricted manner, with mass amounts of sensitive information about U.S. persons continuing to flow to a foreign entity aligned with the PRC and subject to their data collection authorities, and with new users continuing to sign up and have their data exposed. *Cf. Metromedia, Inc. v. City of San Diego*, 453 U.S. 490, 508 (1981) (“If the city has a sufficient basis for believing that billboards are traffic hazards and are unattractive, then obviously the most direct and perhaps the only effective approach to solving the problems they create is to prohibit them.”).

Plaintiffs do not advance their argument by identifying possible alternative approaches that (in their view) would have restricted less speech—*e.g.*, by relying on possible mitigations allegedly posed during CFIUS negotiations, *see* Pls.’ Br. at 29. Such alternative approaches are irrelevant to the analysis. *See Albertini*, 472 U.S. at 689 (“Nor are such regulations invalid simply because there is some imaginable alternative that might be less burdensome on speech.”); *Clark*, 468 U.S. at 299. The First Amendment does not provide Plaintiffs with a license to dictate how the President

may respond to an emerging national-security threat—*i.e.*, foreclosing a robust response, and instead requiring a piecemeal response relying solely on the divestiture order. *Cf. Trump v. Hawaii*, 138 S. Ct. 2392, 2421 (2018) (“[W]e cannot substitute our own assessment for the Executive’s predictive judgments on such matters, all of which are delicate, complex, and involve large elements of prophecy.”).

Nor can Plaintiffs succeed by demanding “supporting evidence” that the Government’s asserted harms are “real.” Pls.’ Br. at 29. Even if strict scrutiny were to apply, the Supreme Court has made clear that the Executive Branch is not required to prove its findings with detail or evidence. *See Humanitarian Law Project*, 561 U.S. at 34-35 (describing such a requirement as “dangerous”); *see also Reno v. Am.-Arab Anti-Discrimination Comm.*, 525 U.S. 471, 490-91 (1999). In any event, a fair reading of the Executive Order makes plain that the President’s identified harms are not speculative. *See TikTok Order*, pmb. (“These risks are real. . . . The United States must take aggressive action against the owners of TikTok to protect our national security.”); *see also Commerce Decision Memo*, at 19-21.

Finally, the Secretary’s restrictions also leave open ample alternative modes of communication, and Plaintiffs do not contend otherwise. *See Pls.’ Br.* at 29-30. Accordingly, even if the Government’s actions were subject to First Amendment scrutiny, they would be sustained as reasonable “time, place, or manner” restrictions.<sup>9</sup>

---

<sup>9</sup>The recent decision in *WeChat Users Alliance v. Trump*, No. 20-cv-5910 (N.D. Cal.), ECF No. 59 (Sept. 19, 2020), does not support Plaintiffs’ claims here. The Government respectfully submits that decision was incorrect because, *inter alia*, it failed to address the threshold question whether First Amendment scrutiny is even warranted; incorrectly faulted the Government for failing to submit detailed evidence supporting its national-security justification; and misconstrued the tailoring inquiry by focusing on potential alternatives, rather than whether the Government’s action was effective in advancing its interests. In any event, that decision was also based on the particular factual record associated with WeChat, involving an “un-phased” set of prohibited transactions, *see id.* at 17, which does not help Plaintiffs here.

**D. The Challenged Actions Do Not Violate Procedural Due Process**

Plaintiffs' claims under the Due Process Clause fail for two reasons. First, with respect to Plaintiffs' challenge to Paragraph 1 of the Secretary's Identification (the only set of prohibitions currently at issue in this motion), Plaintiffs have not established any cognizable liberty or property interests. "Property interests . . . are not created by the Constitution," but instead "are created and their dimensions are defined by existing rules or understandings that stem from an independent source such as state law[.]" *Bd. of Regents of State Colleges v. Roth*, 408 U.S. 564, 577 (1972). Here, Plaintiffs cite no authority demonstrating "a legitimate claim of entitlement," *id.*, to a property interest in having TikTok available on mobile application stores for new users to download and/or for existing users to receive automatic updates. At most, Plaintiffs claim a desire to continue to expand their business, but such "unilateral expectation[s]" generally do not qualify as a protected property interest. *Id.*; *see also Classic Cab, Inc. v. Dist. of Colum.*, 288 F. Supp. 3d 218, 225 (D.D.C. 2018) ("Businesses generally do not have property interests in their assets or revenues. Those are 'incidents' to ownership—goals that are far from guaranteed, and certainly not guaranteed by the government.").

Second, Plaintiffs cannot demonstrate that they were entitled to any additional process. "The Constitution does not grant to members of the public generally a right to be heard by public bodies making decisions of policy." *Minn. State Bd. for Cmty. Colls. v. Knight*, 465 U.S. 271, 283 (1984); *see also Bi-Metallic Inv. Co. v. State Bd. of Equalization*, 239 U.S. 441, 445 (1915). Here, the Executive Orders provide ample reasons on their face demonstrating the reasons for the policy; the legislative structure of IEEPA and the NEA provides Congressional oversight; and the nature of the policy judgment at issue precludes any entitlement to additional process. *See Morrissey v. Brewer*, 408 U.S. 471, 481 (1972) ("[D]ue process is flexible and calls for such procedural protections as the particular situation demands."). Suggesting the President must provide pre-

deprivation notice before declaring a national emergency that may result in prohibited transactions would be a significant constraint on Executive authority. *See* Pls.’ Br. at 30. And to the extent Plaintiffs believe that their materials submitted as part of the CFIUS negotiations are relevant to the Secretary’s exercise of IEEPA authority, *see id.* at 22, Plaintiffs make no effort to explain why the CFIUS negotiations do not themselves provide adequate process and opportunity to rebut the Government’s national-security concerns.

Again, this case is fundamentally different from the cases involving Department of Treasury designations on which Plaintiffs rely, *see* Pls.’ Br. at 31. In those cases, the only question before the agency is whether an entity meets certain criteria for inclusion on the List of Specially Designated Nationals and Blocked Persons. Here, the President exercised a broad policy judgment about the risks posed by TikTok, and similarly the Secretary made a legislative judgment about how best to address those risks. In the context of policy judgments such as these (rather than individualized fact-finding), the nature of the decision precludes any entitlement to additional process.

#### **E. The President’s Actions Are Otherwise Consistent with IEEPA**

Plaintiffs bring one final claim asserting that both the *Commerce Identification* and the President’s TikTok Order are unlawful under IEEPA. As an initial matter, there is no basis for a claim directly against the TikTok Order, because no equitable relief, let alone the preliminary equitable relief at issue here, is available against the President in his official capacity. Federal courts have “no jurisdiction . . . to enjoin the President in the performance of his official duties.” *Mississippi v. Johnson*, 71 U.S. 475, 501 (1866); *see Franklin*, 505 U.S. at 802-03, 806 (plurality op.); *id.* at 827 (Scalia, J., concurring in part and concurring in the judgment) (“apparently unbroken historical tradition supports the view” that courts may not order the President to “perform particular executive . . . acts”). Moreover, Plaintiffs fail to identify any cause of action allowing

them to bring these claims, and IEEPA does not itself contain a private right of action.

In any event, Plaintiffs' argument is meritless. The TikTok Order expressly states that the "additional steps" being ordered are in connection with "the national emergency . . . declared in Executive Order 13873 of May 15, 2019." TikTok Order, pmb. The fact that the President determined that the TikTok restrictions were encompassed within his prior declaration of emergency should be the end of the matter. *See California v. Trump*, 407 F. Supp. 3d at 890-91 (N.D. Cal. 2019) (holding that national emergency determinations are "nonjusticiable political questions").

Moreover, this result is confirmed by the ICTS Order itself, which applies to "information and communications technology or services" and then defines that term broadly: "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display[.]" ICTS Order, § 3(c). Here, TikTok plainly qualifies as a "product or service primarily intended to fulfill . . . communication by electronic means." *Id.* And for the reasons explained above, Plaintiffs are incorrect to assert that the President failed to identify any actual threat posed by TikTok to U.S. national security. *See* Pls.' Br. at 32. Thus, there is no plausible claim challenging the TikTok Order under IEEPA.

## **II. Plaintiffs Have Not Proven Immediate, Urgent Irreparable Harm Justifying a Preliminary Injunction**

The D.C. Circuit "has set a high standard for irreparable injury." *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006). "Such injury must be 'both certain and great,' 'actual and not theoretical,' 'beyond remediation,' and 'of such imminence that there is a clear and present need for equitable relief to prevent irreparable harm.'" *Mexichem Specialty Resins, Inc. v. EPA*, 787 F.3d 544, 555 (D.C. Cir. 2015) (citing *Chaplaincy of Full Gospel*

*Churches*, 454 F.3d at 297).

In general, there are two broad flaws with Plaintiffs' claimed irreparable harm. First, although Plaintiffs describe their claimed harms in a variety of different ways ("market erosion," "reputation," and "competitive strength," Pls.' Br. at 34-35), Plaintiffs are largely just claiming economic harm. Such harm only constitutes irreparable harm, however, "where the loss threatens the very existence of the movant's business." *Wis. Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1984). "The universe of harms that meet this litmus test is narrow indeed." *Econ. Research Servs., Inc. v. Resolution Econ., LLC*, 140 F. Supp. 3d 47, 53 (D.D.C. 2015).

Second, many of Plaintiffs' claimed harms stem from independent decisions of third-parties not before the Court. But "uncertainty" felt by third-parties and their corresponding decisions about how to respond to that uncertainty is not fairly traceable to the Government's actions, nor would any such claimed harms even be redressed if the Court were to enter Plaintiffs' requested relief. That is particularly true given that Plaintiffs do not challenge the President's August 14 divestiture order in this lawsuit, which will independently create lingering uncertainty about TikTok's future even if this Court enters a preliminary injunction for Plaintiffs.

In short, Plaintiffs have not explained how their claimed harms are both irreparable and redressable by the preliminary injunction requested from this Court. The failure to prove both these elements is even more stark when evaluating Plaintiffs' claimed harms in the context of the Paragraph 1 prohibition, which is the subject of the present motion.

First, with respect to economic harm, TikTok asserts a \$10 million loss in advertising revenue in August, Pappas Decl. ¶ 24, but offers no detail to suggest that such a loss represents an "existential" threat to the company. TikTok's motion and Ms. Pappas's declaration are notably silent as to the company's revenues, costs, assets, liabilities, or other line items that would allow

the Court to gauge the overall economic condition of TikTok and the potential effect of the Executive Order and set of prohibited transactions. Indeed, \$10 million appears to be a very small part of ByteDance and TikTok's overall finances. *See Commerce Decision Memo*, at 4 (ByteDance is valued between \$78 billion and \$100 billion); Mike Vorhaus, *ByteDance, Chinese Digital Giant And Owner Of TikTok, Reported To Have Revenues Of \$17 Billion*, *Forbes*, May 28, 2020.<sup>10</sup> The Court should reject these assertions of harm when the only amounts specified in TikTok's papers are dwarfed in comparison to the company's wealth. *See Econ. Research Servs.*, 140 F. Supp. 3d at 53 ("Given the size and prominence of ERS's parent corporation, and the apparent strength of its own infrastructure, this Court has no reason to believe that ERS's alleged losses threaten the company's very existence."); *Ajilon Prof'l Staffing, PLC v. Kubicki*, 503 F. Supp. 2d 358, 362 & n.6 (D.D.C. 2007) (declining to find irreparable harm where the plaintiff, itself a sizeable corporation, was a subsidiary of one of the "world's largest human resource solution providers").<sup>11</sup>

Moreover, given that this harm already occurred in August, there is no reason to believe it was in any way connected to the Secretary's adoption of specific business-to-business transactions (let alone the first prohibition specifically). Nor is there any reason to believe that a preliminary injunction would avoid similar harm going forward, particularly if it was limited only to the Secretary's first prohibition.

As to the first prohibition, TikTok asserts that "the direct effect of the first Prohibition is to halt the influx of new users to TikTok," but that argument is based on TikTok's speculation that

---

<sup>10</sup> Available at <https://www.forbes.com/sites/mikevorhaus/2020/05/27/bytedance-chinese-digital-giant-and-owner-of-tiktok-reported-to-have-revenues-of-17-billion/#71e1948623de>

<sup>11</sup> Without developing the point, TikTok contends that "when sovereign immunity bars a plaintiff from recovering damages from a federal agency—as is the case here—economic loss suffered by the plaintiff *may* be irreparable[.]" Pls.' Mot. at 36 (emphasis added). But regardless of sovereign immunity, TikTok must establish "certain, great and actual" losses, *Nat'l Min. Ass'n v. Jackson*, 768 F. Supp. 2d 34, 52-53 (D.D.C. 2011), which it has failed to do.

“hundreds of millions of U.S. citizens who have not yet downloaded TikTok”—*i.e.*, approximately two thirds of U.S. citizens—are interested in doing so. Pls.’ Br. at 34. TikTok also overlooks the possibility that those interested in downloading TikTok may have already done so since the President issued the Executive Order or the Secretary adopted the prohibitions. *See id.*

At most, allowing the first set of prohibitions to go into effect would only delay the ability of new users to download the application if Plaintiffs were ultimately to prevail in this action. Plaintiffs have not demonstrated that if a user is unable to download TikTok on September 28, 2020, that such user would be lost forever even if Plaintiffs were ultimately to prevail in this action. And more generally, Plaintiffs have submitted no evidence that preventing new users from being able to download TikTok would constitute an existential threat to the company, particularly over a short amount of time (*e.g.*, the amount of time that a temporary restraining order or preliminary injunction would be in effect).

Plaintiffs’ other cited harms are likewise overblown and/or speculative. Plaintiffs state that its content creators are “beginning to build relationships with competing platforms,” and cites the example of one its largest content creators, Charli D’Amelio. *See* Pappas Decl. ¶ 22 & n.3. But Plaintiffs omit the fact that Ms. D’Amelio’s deal with Triller (another social media platform) is not exclusive (meaning she can still post content to TikTok, as well as You Tube and Instagram), and Plaintiffs’ own cited article also notes “almost any creator [will] tell you it’s better to be everywhere instead of on just one app.” TikTok’s contention that it will lose employees and be unable to staff positions is likewise conjectural; the company vaguely asserts that 52 individuals have recently declined TikTok offers “due to the perceived uncertainty caused by the government’s investigation of and threats against TikTok.” *Id.* ¶ 26. The company does not indicate, however, whether 52 is a relatively high or low number, and in any event, TikTok does not explain why a

preliminary injunction here would improve hiring and staff retention. *See id.* (noting that TikTok has to “compete fiercely” to attract talent in the first place); *see also Mead Johnson Pharmaceutical Group v. Bowen*, 665 F. Supp. 53-56 (D.D.C. 1986) (rejecting as “pure speculation” a pharmaceutical company’s claim in support of its preliminary injunction motion that it would suffer loss of sales if a competing generic drug were approved and marketed), *aff’d*, 838 F.2d 1332 (D.C. Cir. 1988); *Wisconsin Gas*, 758 F.2d at 674 (“Bare allegations of what is likely to occur are of no value since the court must decide whether the harm will *in fact* occur.”); *Berman v. DePetrillo*, No. CIV. A. 97-70 (TAF), 1997 WL 148638, at \*2 (D.D.C. Mar. 20, 1997) (“[T]he plaintiffs may hope that some of these ‘industry players’ will team up with them to manufacture and market SAM, but they cannot be certain that any of them will do so.”). *Cf. Arpaio v. Obama*, 797 F.3d 11, 21 (D.C. Cir. 2015) (“When considering any chain of allegations for standing purposes, we may reject as overly speculative those links which are predictions of future events (especially future actions to be taken by third parties), as well as predictions of future injury that are not normally susceptible of labelling as ‘true’ or ‘false.’”).

Finally, Plaintiffs also do not advance their argument by claiming that “Plaintiffs face an immediate restriction of their protected First Amendment rights to speak and receive information.” Pls.’ Mot. at 38. But Plaintiffs’ First Amendment rights have not been violated, as discussed above. And Plaintiffs’ theory fails because they have not demonstrated “*purposeful* unconstitutional suppression of speech [that] constitutes irreparable harm for preliminary injunction purposes.” *CTIA - The Wireless Ass’n v. City of Berkeley*, 928 F.3d 832, 851 (9th Cir. 2019) (citation omitted); *accord Hohe v. Casey*, 868 F.2d 69, 73 (3d Cir. 1989) (“[I]t is the ‘direct penalization, as opposed to incidental inhibition, of First Amendment rights [which] constitutes irreparable injury.’” (citation omitted)). Indeed, the cases on which Plaintiffs rely reveal the comparative weakness of

their claim of irreparable harm. *See Elrod v. Burns*, 427 U.S. 347, 350 (1976) (considering “loss of First Amendment freedoms” arising from alleged discharge on the basis of political leanings); *Grace v. District of Columbia*, 187 F. Supp. 3d 124, 149 (D.D.C. 2016) (Second Amendment challenge to “good reason” requirement to carry concealed firearm).

### **III. The Balance of the Equities and Public Interest Strongly Favor the Government**

Even if Plaintiffs could demonstrate some cognizable harm, the balance of the equities tips sharply in favor of the Government. At issue is a formal national security and foreign affairs determination made by the President, pursuant to an emergency declaration, as authorized by Congress. These interests weigh strongly against an injunction. *See Winter*, 555 U.S. at 24; *Virginian Ry. Co. v. Sys. Fed’n No. 40*, 300 U.S. 515, 552 (1937) (statutory scheme “is in itself a declaration of public interest and policy which should be persuasive” to courts). The injunction Plaintiffs seek would frustrate and displace the President’s determination of how best to address threats to national security. *Milena Ship Mgmt. Co. v. Newcomb*, 804 F. Supp. 846, 854 (E.D. La. 1992) (holding that injunction “unblocking the plaintiffs’ vessels and bank accounts before a full hearing on the merits of OFAC’s blocking decisions would risk impermissible interference with Executive and Congressional decisions”).

Plaintiffs criticize the timing of the Government’s actions, asserting that the delay in enforcing the prohibitions suggests the Government’s interests are not serious. *See Pls.’ Br.* at 37. But decisions regarding how to address threats from abroad “involve significant political ramifications[,]” and, “[a]ccordingly, the Court must defer to the Executive’s discretion on the timing of those . . . decisions.” *Holy Land Found. for Relief & Dev.*, 219 F. Supp. 2d at 74 n.28. Moreover, the logic of this argument would effectively preclude the Government from enacting calibrated, strategic measures; Plaintiffs’ approach would effectively require the Executive Branch to respond to every national-security threat with full force, or else risk having its judgments

second-guessed by courts.

The Court here must grant deference to the Executive’s “evaluation of the facts” and the “sensitive and weighty interests of national security and foreign affairs.” *Humanitarian Law Project*, 561 U.S. at 33-34. Even if Plaintiffs established some modicum of harm, therefore, those “weighty interests” ensure that the equitable balance squarely favors the Government and is an independent reason for denying relief. *Cf. Def. Distributed v. Dep’t of State*, 838 F.3d 451, 458-60 (5th Cir. 2016) (Government’s interests in national defense and national security outweighed potential temporary infringement of plaintiffs’ constitutional rights).

#### **IV. Any Relief Should Be Appropriately Limited, and Require Posting of a Bond**

To the extent the Court is inclined to grant relief, the remedy “must be tailored to redress the plaintiff’s particular injury,” *Gill v. Whitford*, 138 S. Ct. 1916, 1934 (2018), and “injunctive relief should be no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs.” *Madsen v. Women’s Health Ctr., Inc.*, 512 U.S. 753, 765 (1994). Here, the Court should ensure that any preliminary relief entered is based on a specific showing of irreparable harm with respect to paragraph 1 of the *Commerce Identification*, and that the preliminary relief extends no further than is necessary to redress that particular form of demonstrated irreparable harm. Any decision regarding the other paragraphs of the *Commerce Identification* should appropriately be the subject of separate proceedings, which could be briefed and decided prior to those restrictions’ effective date of November 12, which is the Government’s understanding of these proceedings as discussed during the September 24 scheduling hearing. *See* Hr’g Tr. at 21 (“[T]he immediate issue before me, as I see it, is whether September 27th, whether Paragraph 1 should be permitted to take effect or should be enjoined.”).

Additionally, to the extent the Court orders preliminary relief against Paragraph 1, the Government believes it would be appropriate to require Plaintiffs to post a bond pursuant to Fed.

R. Civ. P. 65(c). “It is well settled that Rule 65(c) gives the Court wide discretion in the matter of requiring security.” *Fox Television Stations, Inc. v. FilmOn X LLC*, 966 F. Supp. 2d 30, 52 (D.D.C. 2013). Here, any relief would impose “material damage” on Defendants, *id.*, by interfering with a formal national security judgment of the President; altering the landscape with respect to ongoing CFIUS negotiations; and continuing to allow sensitive and valuable user information to flow to ByteDance with respect to all new users who download TikTok while the preliminary injunction remains in effect. This last item in particular is reasonably capable of monetization, and the Court should, at a minimum, order Plaintiffs to post a bond commensurate with the value of the user information that would continue flowing to ByteDance as a result of any preliminary relief entered in this case.

### CONCLUSION

This Court should deny Plaintiffs’ motion for a preliminary injunction.

Dated: September 25, 2020

Respectfully submitted,

JEFFREY BOSSERT CLARK  
Acting Assistant Attorney General

AUGUST FLENTJE  
Special Counsel to the Acting  
Assistant Attorney General

ALEXANDER K. HAAS  
Branch Director

DIANE KELLEHER  
Assistant Branch Director

/s/ Daniel Schwei

DANIEL SCHWEI

Special Counsel

SERENA M. ORLOFF

MICHAEL DREZNER

AMY E. POWELL

STUART J. ROBINSON

Trial Attorneys  
United States Department of Justice  
Civil Division, Federal Programs Branch  
Ben Franklin Station, P.O. Box No. 883  
Washington, DC 20044  
Phone: (202) 305-8693  
Fax: (202) 616-8470  
E-mail: daniel.s.schwei@usdoj.gov

*Counsel for Defendants*