



4-1-2021

Political Posturing or a Move Towards "Net Nationalism?" The Legality of a TikTok Ban and Why Foreign Tech Companies Should Be Paying Attention

Gabrielle Supak

Follow this and additional works at: <https://scholarship.law.unc.edu/ncjolt>



Part of the [Law Commons](#)

Recommended Citation

Gabrielle Supak, *Political Posturing or a Move Towards "Net Nationalism?" The Legality of a TikTok Ban and Why Foreign Tech Companies Should Be Paying Attention*, 22 N.C. J.L. & TECH. 527 (2021).

Available at: <https://scholarship.law.unc.edu/ncjolt/vol22/iss3/6>

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of Law & Technology by an authorized editor of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.

POLITICAL POSTURING OR A MOVE TOWARDS “NET NATIONALISM?”: THE LEGALITY OF A TIKTOK BAN AND WHY FOREIGN TECH COMPANIES SHOULD BE PAYING ATTENTION

*Gabrielle Supak**

In July 2020, former President Trump issued an Executive Order attempting to unilaterally ban TikTok, a social media platform used mainly by teenagers to post videos of dances or viral challenges. Banning a social media app is unprecedented in the United States and raises various concerns among a wide variety of interested parties. These concerns range from whether the President could legally take such action to whether First Amendment rights were violated to simply why even target a seemingly nonsensical social media app. This Article attempts to answer these questions and provides guidance to foreign tech companies that wish to continue doing business in a United States that glaringly disapproves of any company with ties to the government of the People’s Republic of China.

TABLE OF CONTENTS

I.	INTRODUCTION.....	528
II.	LEGAL FRAMEWORK	531
	<i>A. International Emergency Economic Powers Act.....</i>	<i>531</i>
	1. <i>The Informational Materials Amendment Limitation..</i>	<i>535</i>
	2. <i>National Security Exemption from Compliance</i>	<i>538</i>
	<i>B. Committee on Foreign Investment in the United States.....</i>	<i>540</i>
	<i>C. Entity List.....</i>	<i>544</i>

* J.D. Candidate, University of North Carolina School of Law, 2022. The Author would like to thank all of the JOLT staff for their assistance on this Article, especially Andy Tabeling, Alessandra Carlton, and Jasmine Washington for their dedication to this piece. The Author would also like to thank her family and friends for their unwavering support, especially her grandparents, who have always supported her goal of becoming an attorney. Lastly, the Author would like to thank her dog, Maggie, for being the best companion throughout the development of this piece.

III.	IMPLICATIONS OF A BAN ON FIRST AMENDMENT RIGHTS....	546
	<i>A. First Amendment Rights of TikTok Content Creators and Users</i>	<i>547</i>
	1. <i>Content-Based Restrictions.....</i>	<i>548</i>
	2. <i>Content-Neutral Restrictions</i>	<i>551</i>
	<i>B. First Amendment Rights of Platform Owners in their Source Code</i>	<i>551</i>
	<i>C. Balancing the First Amendment and National Security.....</i>	<i>553</i>
	1. <i>TikTok Ban as a Content-Neutral Restriction.....</i>	<i>556</i>
	2. <i>Applying the Terrorism Approach to Cyber-Espionage.....</i>	<i>557</i>
IV.	TIKTOK AS AN EXAMPLE FOR OTHER FOREIGN TECH AND APP COMPANIES.....	558
	<i>A. The U.S. Clean Network Initiative and its Effects</i>	<i>559</i>
	<i>B. Sanctions as an Alternative to the Clean Network</i>	<i>563</i>
	<i>C. Movement Toward a “Splinternet”</i>	<i>564</i>
	<i>D. The Biden Administration’s Approach</i>	<i>566</i>
	<i>E. Possible Solutions</i>	<i>568</i>
V.	CONCLUSION	571

I. INTRODUCTION

On July 31, 2020, President Trump boldly proclaimed to reporters aboard Air Force One that “[a]s far as TikTok is concerned we’re banning them from the United States.”¹ At first glance, many may wonder why the President of the United States would want to ban an app² used primarily by teenagers and young adults.³ Going back to 2018, TikTok was introduced as a popular video creating

¹ Maggie Haberman (@maggieNYT), TWITTER (July 31, 2020, 10:29 PM), <https://twitter.com/maggieNYT/status/1289387767059775489> [<https://perma.cc/X8YT-QS5U>].

² “App” is short for application. An application is the same thing as a software program. Apple popularized the term “app” with the creation of its “App Store” in 2008. *App*, TECHTERMS (Sept. 22, 2012), <https://techterms.com/definition/app#:~:text=The%20term%20%22app%22%20was%20popularized,to%20refer%20to%20mobile%20applications> [<https://perma.cc/DZ3E-E3Q9>].

³ See Katie Sehl, *20 Important TikTok Stats Marketers Need to Know in 2020*, HOOTSUITE BLOG (May 7, 2020), <https://blog.hootsuite.com/tiktok-stats/> [<https://perma.cc/5N6C-BNLH>].

and sharing platform.⁴ By 2020, TikTok had over 800 million global users and was the sixth most used social app in the world.⁵ TikTok's popularity led to unprecedented growth in the United States.⁶ For example, in February 2019, there were 26,739,143 monthly active users in the United States.⁷ By August 2020, 100 million Americans were using TikTok, half of whom were considered daily users.⁸ However, the problem for President Trump was that TikTok is owned by ByteDance, a Chinese tech company.⁹

On August 6, 2020, President Trump followed through on what he told reporters aboard Air Force One.¹⁰ Trump issued an Executive Order prohibiting “any transaction by any person, or with respect to any property, subject to the jurisdiction of the United States, with ByteDance Ltd.”¹¹ The President cited concerns that TikTok threatened “the national security, foreign policy, and economy of the United States.”¹² Specifically, President Trump suggested that TikTok's “data collection threatens to allow the Chinese Communist Party access to Americans’ personal and proprietary information—potentially allowing China to track the locations of federal employees and contractors, build dossiers of personal information

⁴ John Herrman, *How TikTok is Rewriting the World*, N.Y. TIMES (Mar. 10, 2019), <https://www.nytimes.com/2019/03/10/style/what-is-tik-tok.html?auth=linked-facebook> [https://perma.cc/P94M-D6YN].

⁵ Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2020)*, BUS. OF APPS (Oct. 15, 2020), <https://www.businessofapps.com/data/tik-tok-statistics/> [https://perma.cc/RK6H-DSZ5].

⁶ Complaint at 6, *TikTok, Inc. v. Trump*, No. 2:20-cv-7672 (C.D. Cal. 2020).

⁷ *Id.*

⁸ *Id.* at 6–7.

⁹ Bobby Allyn, *Will TikTok Be Banned in The USA? It May Depend On Who Owns It*, NPR (July 23, 2020, 11:34 AM), <https://www.npr.org/2020/07/23/894351718/will-tiktok-be-banned-in-the-usa-it-may-depend-on-who-owns-it#:~:text=The%20Trump%20administration%20is%20considering,the%20Chinese%20technology%20giant%20ByteDance> [https://perma.cc/H26D-ZHYR].

¹⁰ Haberman, *supra* note 1; Bobby Allyn, *Trump Signs Executive Order That Will Effectively Ban Use of TikTok in the U.S.*, NPR (Aug. 6, 2020, 11:21 PM), <https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s> [https://perma.cc/9JA5-C23H].

¹¹ Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 6, 2020).

¹² *Id.*

for blackmail, and conduct corporate espionage.”¹³ TikTok quickly responded to President Trump’s Executive Order and filed a lawsuit on August 24, 2020.¹⁴ In this Executive Order challenge, TikTok alleged that President Trump’s Executive Order went beyond his presidential powers, along with many other constitutional complaints.¹⁵

Despite the Executive Order’s unprecedented nature,¹⁶ banning TikTok using the existing legal framework that regulates international trade is a valid, albeit nontraditional, approach. Therefore, foreign tech and app companies, especially those perceived to be under the Chinese government’s influence, should prepare for the age of “net nationalism”¹⁷ if they want to continue doing business in the United States.¹⁸

This Article proceeds in four parts. Part II examines the legal framework in place that allows bans of foreign apps and other tech, including the International Emergency Economic Powers Act, the Committee on Foreign Investment in the United States, and the Commerce Department’s Entity List. Part III looks at the First Amendment implications of such a ban, including whether TikTok has First Amendment protections, along with a counterargument that legitimate government interests in protecting national security outweigh any First Amendment interests TikTok may have. Finally, Part IV argues that the ban implicates numerous international tech concerns, including the rise of net nationalism, the creation of the U.S. Clean Network, and what actions tech companies should take to alleviate national security fears.

¹³ *Id.*

¹⁴ Complaint, *supra* note 6, at 1.

¹⁵ *See generally id.* TikTok alleged constitutional violations of the First Amendment, due process protections of the Fifth Amendment, and a taking without compensation in violation of the Fifth Amendment.

¹⁶ Banning TikTok is unprecedented because after extensive research, it appears that a U.S. president has never unilaterally banned a mobile app like TikTok.

¹⁷ “Net Nationalism” is the idea of governments using the internet as a tool to promote nationalistic policies and goals; thus, prioritizing the goals of one’s country over the goals of a globally connected world. *See* Tim Wu, *A Tik Tok Ban is Overdue*, N.Y. TIMES (Aug. 18, 2020), <https://www.nytimes.com/2020/08/18/opinion/tiktok-wechat-ban-trump.html> [<https://perma.cc/G625-DWUW>].

¹⁸ *Id.*

II. LEGAL FRAMEWORK

In issuing the August 6th Executive Order, President Trump cited the International Emergency Economic Powers Act and the National Emergencies Act to support his authority to prohibit transactions with ByteDance.¹⁹ The Executive Order also relied on findings from a review conducted by the Committee on Foreign Investment in the United States (“CFIUS”). However, there are other methods President Trump could have used to accomplish this goal. Alternatively, President Trump could have achieved a similar outcome by solely relying on a CFIUS review or placing TikTok on the U.S. Commerce Department’s Entity List.²⁰ These three executive branch options, beginning with the route President Trump took, are discussed in detail below.

A. *International Emergency Economic Powers Act*

The International Emergency Economic Powers Act (“IEEPA”)²¹ is an emergency statute located within the umbrella of the National Emergencies Act (“NEA”).²² NEA was a response to a committee study that aimed “to identify any states of national emergency that were still in effect and to determine the universe of federal statutes that bestow on the president special powers in such situations.”²³ NEA did not change what powers are granted to a president during a national emergency.²⁴ Instead, the statute created a process for Congress to terminate a presidential emergency declaration.²⁵ IEEPA is one of approximately 475 statutes that grant

¹⁹ Exec. Order No. 13942, *supra* note 11.

²⁰ Paige Leskin, *No, Donald Trump Really Can’t ‘Ban’ TikTok*, BUS. INSIDER (Aug. 5, 2020, 8:47 AM), <https://www.businessinsider.com/can-trump-ban-tiktok-no-legal-experts-cfius-alternative-options-2020-7> [<https://perma.cc/BZE2-UDVB>].

²¹ 50 U.S.C. § 1702.

²² CHRISTOPHER A. CASEY ET AL., CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 2 (2020).

²³ James Wallner, *The National Emergencies Act of 1976*, LEGBRANCH.ORG (Feb. 28, 2019), <https://www.legbranch.org/the-national-emergencies-act-of-1976/> [<https://perma.cc/U35Y-33TY>].

²⁴ *Id.*

²⁵ *Id.*

the president emergency powers following a national emergency declaration.²⁶

Invoking IEEPA allows the president “to investigate, regulate, or prohibit foreign exchange transactions, transfers of credit, transfers of securities, payments, and . . . take specified actions relating to property in which a foreign country or person has interest.”²⁷ The President may “freez[e] assets, block[] property and interests in property, prohibit[] U.S. persons from entering into transactions related to frozen assets and blocked property, and in some instances deny[] entry into the United States.”²⁸

For the IEEPA provision to be triggered, the President must first declare a national emergency or link the situation to a previously declared national emergency.²⁹ Here, President Trump linked TikTok to the previously issued Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain.³⁰ President Trump asserted that Executive Order 13873 was issued and created a national emergency because

Foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.³¹

Executive Order 13873 was initially issued to target foreign telecommunications companies, including Chinese tech giants Huawei and ZTE.³²

²⁶ *Id.*

²⁷ CASEY ET AL., *supra* note 22, at 26.

²⁸ *Id.*

²⁹ *Id.*

³⁰ Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019).

³¹ *Id.*

³² Eric Geller, *Trump Signs Order Setting Stage to Ban Huawei from U.S.*, POLITICO (May 15, 2019, 7:05 PM), <https://www.politico.com/story/2019/05/15/trump-ban-huawei-us-1042046> [<https://perma.cc/B8XJ-2V3Y>]. Huawei and ZTE, like TikTok, were targeted because of security fears that they would enable foreign adversaries to spy on the U.S. through the implementation of their 5G networks. *Id.*

IEEPA makes it possible to “deplatform” an app, which is one of the most extreme routes the Trump administration could have taken to ban TikTok.³³ Although deplatforming has traditionally been the “removal of one’s account for breaking platform rules,”³⁴ the term would apply here because TikTok would be removed from app stores that are not up to par with U.S. national security standards as outlined in the Executive Order.³⁵ By citing IEEPA, the TikTok Executive Order can deplatform the app because “[i]f the act is enforced, Americans would stop seeing TikTok in app stores and would not be able to download software updates, eventually rendering the social media app useless.”³⁶

President Trump planned to begin to ban TikTok (along with Chinese app WeChat) on Sunday, September 20, 2020, and intended to later widen restrictions on November 12, 2020.³⁷ Initially, the proposed ban would have meant users could not download or update the app.³⁸ However, the later widened restrictions would have prohibited any transaction involving internet hosting, content delivery network services, directly contracted or arranged internet transit or peering services, and any utilization of TikTok’s mobile

³³ Adi Robertson, *How the Trump Administration Could ‘Ban’ TikTok*, THE VERGE (Aug. 1, 2020, 12:12 AM), <https://www.theverge.com/2020/7/9/21315983/trump-pompeo-ban-tiktok-bytedance-chinese-social-media-national-security-censorship-methods> [<https://perma.cc/8A2N-99AC>].

³⁴ Richard Rogers, *Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media*, *European Journal of Communication*, 35 EUR. J. OF COMM. 213, 214 (2020) (discussing how extreme internet celebrities such as Alex Jones and Milo Yiannopoulos have been removed from major social media platforms for engaging in dangerous, extreme speech).

³⁵ Exec. Order No. 13942, *supra* note 11.

³⁶ *Trump Signs Executive Order Essentially Banning U.S. Companies from Working with TikTok*, FIRST AMENDMENT WATCH AT NYU (Aug. 7, 2020), <https://firstamendmentwatch.org/trump-signs-executive-order-essentially-banning-u-s-companies-from-working-with-tiktok/> [<https://perma.cc/VHS5-26LZ>].

³⁷ Ana Swanson et al., *Trump Administration to Ban TikTok and WeChat From U.S. App Stores*, N.Y. TIMES (Sept. 18, 2020, 1:47 PM), <https://www.nytimes.com/2020/09/18/business/trump-tik-tok-wechat-ban.html> [<https://perma.cc/B32F-S7NJ>].

³⁸ *Id.*

app constituent code, or software.³⁹ The proposed deplatforming on this scale by the federal government's executive branch should concern any company, foreign or not, that wishes to conduct business in the United States.

Luckily for TikTok and its then 100 million American users, an injunction was issued halting the ban from going into effect after a rare Sunday emergency hearing.⁴⁰ This injunction was a win for ByteDance, which was still negotiating the sale of TikTok to Oracle and Walmart.⁴¹ The Trump Administration set December 4, 2020, as the deadline for negotiations.⁴² However, the deadline quietly passed and was not extended.⁴³ At the time, anonymous sources with knowledge of the matter reported that the U.S. government would not enforce the deadline because the negotiations were ongoing, and the U.S. government was "highly motivated" to reach a resolution.⁴⁴

On December 14, 2020, a panel of judges heard oral arguments concerning the Trump Administration's appeal to reinstate the ban

³⁹ Identification of Prohibited Transactions To Implement Executive Order 13942, 85 Fed. Reg. 60061, 60062 (Sept. 24, 2020) (to be codified at 15 C.F.R. pt. VII).

⁴⁰ Rachel Lerman, *Judge Blocks TikTok Ban in Second Ruling Against Trump's Efforts to Curb Popular Chinese Services*, WASH. POST (Sept. 27, 2020, 9:54 PM), <https://www.washingtonpost.com/technology/2020/09/27/tiktok-ban-injunction/> [<https://perma.cc/S35H-CFA2>].

⁴¹ Vanessa Pappas, *An Update for Our TikTok Family*, TIKTOK (Sept. 19, 2020), <https://newsroom.tiktok.com/en-us/an-update-for-our-tiktok-family> [<https://perma.cc/98HT-ACBN>]. Oracle planned to serve as TikTok's trusted cloud and technology provider responsible for securing user data. *Id.* Oracle and Walmart would be able to take up to a twenty percent cumulative stake in the company following a TikTok Global pre-IPO financing round. *Id.*

⁴² Jay Peters, *The US Government Will Let TikTok Run Out the Clock and 'Overlook' Its Own Deadline*, THE VERGE (Dec. 4, 2020, 9:02 PM), <https://www.theverge.com/2020/12/4/22154801/us-government-tiktok-ban-deadline-bytedance-trump-administration-cfius> [<https://perma.cc/L3BJ-JYQJ>].

⁴³ *Id.*

⁴⁴ *Id.* But see Molly Schuetz, *TikTok sale to Walmart, Oracle Shelved amid Biden Review*: WSJ, BLOOMBERG (Feb. 10, 2021), <https://www.bnnbloomberg.ca/tiktok-sale-to-walmart-oracle-shelved-amid-biden-review-wsj-1.1561756> [<https://perma.cc/MHK3-TUDK>] (reporting that TikTok's sale to Oracle and Walmart has been put on hold pending a review by the Biden Administration).

if the sale was not completed.⁴⁵ Both the district court injunction opinion and the appellate panel of judges⁴⁶ expressed that Trump may have overstepped his authority under IEEPA because of the Personal Communication Limitation⁴⁷ and Informational Materials Amendment Limitation.⁴⁸

1. *The Informational Materials Amendment Limitation*

The Informational Materials Amendment or “Berman Amendment”⁴⁹ excludes “information or informational materials” from IEEPA coverage, including but not limited to publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds, provided such exchange is not otherwise controlled for national security or foreign policy reasons.”⁵⁰ In 1993, the Freedom

⁴⁵ David Yaffe-Bellany, *TikTok Appellate Judges Signal Skepticism of Trump’s Ban on App*, BLOOMBERG (Dec. 14, 2020, 11:37 AM), <https://www.bloomberg.com/news/articles/2020-12-14/tiktok-appeals-court-judges-appear-skeptical-of-trump-ban-on-app> [<https://perma.cc/MG29-MPZD>].

⁴⁶ Oral Argument at 23:50, *TikTok, Inc. v. Trump*, No. 20-5302 (D.C. Cir. Dec. 14, 2020), [https://www.cadc.uscourts.gov/recordings/recordings2020.nsf/31F182605F720B498525863E0064C310/\\$file/20-5302.mp3](https://www.cadc.uscourts.gov/recordings/recordings2020.nsf/31F182605F720B498525863E0064C310/$file/20-5302.mp3) [<https://perma.cc/E99B-SARR>]. U.S. Circuit Judge Judith Rogers rebuked the government’s justification for the ban under the Information Materials Amendment, openly telling the government attorney that “Congress wrote this language, it seems to just fly in the face of that.” *Id.*

⁴⁷ 50 U.S.C. § 1702(b)(1) (stating that IEEPA’s granting of executive authority does not include the “authority to regulate or prohibit, directly or indirectly . . . any . . . personal communication, which does not involve the transfer of anything of value.”). This provision is not explicitly discussed in this paper, however, there are arguments that users on TikTok exchange their data for the ability to use TikTok, which would qualify as a transfer of something of value. If this is the case, then the executive branch is not barred from banning TikTok under IEEPA.

⁴⁸ Memorandum Opinion in Support of Order Granting Plaintiff’s Motion for Preliminary Injunction, *TikTok Inc. v. Trump*, No. 1:20-cv-02658, at 9 (D.D.C. Sept. 27, 2017); Yaffe-Bellany, *supra* note 45.

⁴⁹ 138 CONG. REC. 15,052 (1992). Rep. Howard L. Berman was an advocate of the Informational Materials Amendment and testified to Congress that “[t]he fact that we disapprove of the government of a particular country ought not to inhibit our dialog [sic] with the people who suffer under those governments We are strongest and most influential when we embody the freedoms to which others aspire.” *Id.*

⁵⁰ CASEY ET AL., *supra* note 22, at 12.

to Trade in Ideas Act clarified that information was covered “regardless of format or medium of transmission.”⁵¹ TikTok’s code would, presumably, be covered by the Information Materials Amendment under this definition. The U.S. District Court for Washington, D.C. determined TikTok’s content qualified as informational materials by comparing it to a news wire that is a channel for different types of informational materials.⁵²

Although this Amendment does not explicitly cover digital social media apps, it would be a logical extension of the Amendment considering the similarity between the functions of TikTok compared to what is already covered. The list of covered informational materials includes the phrase “including but not limited to,” which indicates the list is meant to be illustrative and not finite.⁵³ At the time the Amendment was enacted, compact discs were considered a new technology for information storage.⁵⁴ Social media apps, like TikTok, are just a form of new technology used to store informational materials; therefore, just like compact discs, apps fall under the statute’s protection. The fact that TikTok is a digital app is immaterial to this analysis because the Freedom to Trade in Ideas Act clarified that the format or medium of transmission does not affect coverage.⁵⁵

The U.S. government argues that the ban does not run afoul of the Informational Materials Amendment because it claims the proposed ban only regulates business-to-business economic transactions and does not prohibit importing or exporting tangible or intangible informational materials.⁵⁶ The government chooses to differentiate TikTok from the listed examples given in the

⁵¹ See Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525, 108 Stat. 382, 474 (1994).

⁵² Memorandum Opinion, *supra* note 48, at 11.

⁵³ Jarred O. Taylor III, *Information Wants to be Free (of Sanctions): Why the President Cannot Prohibit Foreign Access to Social Media Under U.S. Export Regulations*, 54 W.M. & MARY L. REV. 297, 307 (2012).

⁵⁴ *Id.* at 308.

⁵⁵ See Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525, 108 Stat. 382, 474 (1994).

⁵⁶ Defendant’s Memorandum in Opposition to Plaintiff’s Motion for a Preliminary Injunction, at 17, *TikTok Inc. v. Trump*, No. 1:20-cv-2658 2020 WL 5763634 (D.D.C. Sept. 25, 2020).

Informational Materials Amendment because TikTok's terms of service describe it as a "diverse set of services, that (among other things) manipulates, collects, processes, transmits, brokers, and sells information."⁵⁷

However, the government's terms of service characterization will not suffice to exempt TikTok from being covered by the Informational Materials Amendment because TikTok's central feature is information sharing in the form of short videos.⁵⁸ In contrast, a possible, perhaps even successful argument, for the government, would be to focus on how TikTok users are not using the platform for "free" because users agree to let TikTok collect their valuable data.⁵⁹ Therefore, TikTok's business model could be characterized as a transaction for a service.⁶⁰ If the government took this approach, it is more likely that the Informational Materials Amendment will not protect TikTok because the platform would more closely resemble an economic transaction than the free flow of information. As the government explains, it would be contradictory if Congress gave the President the power to block transactions deemed legitimate national security threats yet allowed those same

⁵⁷ *Id.*

⁵⁸ Paige Leskin, *Inside the Rise of TikTok, the Viral Video-Sharing App Wildly Popular With Teens and Loathed By the Trump Administration*, BUS. INSIDER, (Aug. 7, 2020, 5:20 PM), <https://www.businessinsider.com/tiktok-app-online-website-video-sharing-2019-7> [<https://perma.cc/2FY5-5CVP>].

⁵⁹ TERMS OF SERVICE, TIKTOK <https://www.tiktok.com/legal/terms-of-use?lang=en> [<https://perma.cc/63HMLXRN>] (last updated Feb. 2019) ("We automatically collect certain information from you when you use the Platform, including internet or other network activity information such as your IP address, geolocation-related data (as described below), unique device identifiers, browsing and search history (including content you have viewed in the Platform), and Cookies (as defined below).").

⁶⁰ *Id.*; Justin Sherman, *Unpacking TikTok, Mobile Apps and National Security Risks*, LAWFARE, (Thursday, Apr. 2, 2020, 10:06 AM), <https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks> [<https://perma.cc/APY3-K3RL>] ("It notes further that '[w]e also collect information you share with us from third-party social network providers, and technical and behavioral information about your use of the Platform,' such as, potentially, contact lists on other social media services.").

companies to bypass the executive block by ensuring at least part of its business deals with informational materials.⁶¹

2. *National Security Exemption from Compliance*

Even if the government's above arguments failed, the Informational Materials Amendment would not apply if the exchange is controlled for national security reasons, including weapons proliferation, international terrorism, and espionage.⁶² Although the Trump Administration has claimed national security concerns with TikTok,⁶³ it is unclear whether these concerns rise to the level of exemption from the IEEPA Informational Materials Amendment. The espionage exemption is particularly relevant here because the TikTok Executive Order alleges that the Chinese government is using, or could use, TikTok for espionage purposes.⁶⁴

In a partially redacted Commerce Department memo, government officials explicitly laid out some of these national security concerns.⁶⁵ The memo highlighted the FBI's determination that Chinese "intelligence and economic espionage presents the greatest long-term threat to U.S. national security and economic security."⁶⁶ The memo further claimed that the "bulk" data collection practices that China engages in "is 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

⁶¹ Defendant's Memorandum, *supra* note 56, at 18–19. However, it is important to note, the national security threat must be real. A president should not be able to use the national security exemption to block any transaction under the guise of national security.

⁶² 50 U.S.C. § 1702(b)(3).

⁶³ See Exec. Order No. 13942, *supra* note 11.

⁶⁴ *Id.* (explaining that TikTok's "data collection threatens to allow the Chinese Communist Party 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").

⁶⁵ U.S. Dep't of Com., Memorandum for the Secretary on the Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942 (Sept. 17, 2020), as reprinted in Defendant's Memorandum in Opposition to Plaintiff's Motion for a Preliminary Injunction Exhibit 1, TikTok Inc. v. Trump, No. 1:20-cv-02658, (D.D.C. Sept. 27, 2020).

⁶⁶ *Id.* at 5.

recruitment.”⁶⁷ The Commerce Department also discussed how the Chinese Communist Party (“CCP”) requires party members to be employed by private or non-governmental Chinese organizations.⁶⁸ Most alarmingly, the Commerce Department claimed that Chinese law requires companies subject to its jurisdiction, such as ByteDance, to assist with surveillance and intelligence efforts if requested to do so.⁶⁹

In its injunction opinion, the U.S. District Court for Washington, D.C. considered the government’s espionage argument but called it novel because the relevant espionage section of the U.S. Code “authorizes life imprisonment or the death penalty for those who share U.S. defense secrets . . . with foreign adversaries.”⁷⁰ The court further determined, “it is not plausible that the films, photos, art, or even personal information U.S. users share on TikTok fall within the plain meaning of the Espionage Act.”⁷¹

The government’s espionage argument, however, requires a further analysis of the Espionage Act. The Espionage Act generally seeks to punish those who undermine the “national defense.”⁷² The Supreme Court of the United States construed the term “national defense” as “a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.”⁷³ Here, President Trump identified Chinese

⁶⁷ *Id.* at 6.

⁶⁸ *Id.* at 7. In 2017, seventy percent of private owned companies in China had CCP committees within the organization, including ByteDance. *Id.*

⁶⁹ *Id.* at 9. China’s National Security Law requires that “[a]ny organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law.” National Security Law of the People’s Republic of China Art. 7. The law goes on that state “intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation.” *Id.* at Art. 14. *See also* Daniel Wagner, The Global Implications of China’s National and Cyber Security Laws, *DIPLOMATIC COURIER* (Aug. 7, 2020), <https://www.diplomaticcourier.com/posts/the-global-implications-of-chinas-national-and-cyber-security-laws> [<https://perma.cc/GY6M-LSAW>].

⁷⁰ Memorandum Opinion, *supra* note 48, at 13.

⁷¹ *Id.*

⁷² 18 U.S.C. § 793.

⁷³ *Gorin v. U.S.*, 312 U.S. 19, 28 (1941) (adopting the U.S. Government’s definition of “national security”).

cyber espionage as a threat to the national defense, and thus, banning TikTok because of its compromised position *could* be considered a related activity of national preparedness. This achieves the purpose of national preparedness because IEEPA can be used to “block and prohibit all transactions in all property and interests in property” of people and companies 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.”⁷⁴ Therefore, if the espionage threat was legitimate, then use of IEEPA was proper.

B. Committee on Foreign Investment in the United States

Alternatively, Trump could have solely relied on CFIUS review to “ban” TikTok. In fact, this was the route many experts believed the Trump administration would take.⁷⁵ CFIUS “is an interagency committee with authority to review, block, and where necessary compel divestment of foreign acquisitions of U.S. businesses.”⁷⁶ The Secretary of the Treasury chairs CFIUS, and additional members “include the Secretaries of Homeland Security, Commerce, Defense, State, Energy, and Labor, the Attorney General, the Director of National Intelligence, the U.S. Trade Representative, and the Director of the Office of Science and Technology Policy.”⁷⁷

CFIUS was initially authorized to act pursuant to Section 721 of the Defense Production Act of 1950, also known as the Exon-Florio amendment.⁷⁸ Section 721 has since been revised, first by the Foreign Investment and National Security Act of 2007 (“FINSA”)

⁷⁴ 50 U.S.C. § 1708(b)(1), (2).

⁷⁵ See Leskin, *supra* note 20.

⁷⁶ Geoffrey Gertz, *Why is the Trump Administration Banning TikTok and WeChat?*, BROOKINGS (Aug. 7, 2020), <https://www.brookings.edu/blog/up-front/2020/08/07/why-is-the-trump-administration-banning-tiktok-and-wechat/> [<https://perma.cc/U8T5-6WL3>].

⁷⁷ LATHAM & WATKINS LLP, OVERVIEW OF THE CFIUS PROCESS 1 (2017), <https://www.lw.com/thoughtLeadership/overview-CFIUS-process> [<https://perma.cc/YC89-RK9F>].

⁷⁸ *CFIUS Laws and Guidance*, DEP’T OF TREASURY, <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance> [<https://perma.cc/Q3Q7-74GL>] (last visited Jan. 12, 2021).

and later the Foreign Investment Risk Review Modernization Act of 2018 (“FIRRMA”).⁷⁹ At its inception, CFIUS was only allowed to review transactions that could result in foreign control of a U.S. business.⁸⁰ FIRRMA expanded the jurisdiction of CFIUS to include “non-controlling investments in U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies;⁸¹ own, operate, manufacture, supply, or service critical infrastructure;⁸² or maintain or collect sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security.”⁸³ In this context, “sensitive personal data” is defined as including:

[T]en categories of data maintained or collected by U.S. businesses that (i) target or tailor products or services to certain populations, including U.S. military members and employees of federal agencies with national security responsibilities, (ii) collect or maintain such data on at least one million individuals, or (iii) have a demonstrated business objective to maintain or collect such data on greater than one million individuals and such data is an integrated part of the U.S. business’s primary products or services. The categories of data include types of financial, geolocation, and health data, among others.⁸⁴

When reviewing foreign acquisitions or non-controlling covered investments⁸⁵ in U.S. businesses, the role of CFIUS is to evaluate

⁷⁹ *Id.*; 50 U.S.C. § 4565.

⁸⁰ U.S. DEP’T OF TREASURY, FACT SHEET: FINAL CFIUS REGULATIONS IMPLEMENTING FIRRMA 3 (Jan. 13, 2020), <https://home.treasury.gov/system/files/206/Final-FIRRMA-Regulations-FACT-SHEET.pdf> [<https://perma.cc/7GFL-YBND>].

⁸¹ “CFIUS may review certain transactions involving U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies. ‘Critical technologies’ is defined to include certain items subject to export controls and other existing regulatory schemes, as well as emerging and foundational technologies controlled pursuant to the Export Control Reform Act of 2018.” *Id.*

⁸² “CFIUS may review certain transactions involving U.S. businesses that perform specified functions—owning, operating, manufacturing, supplying, or servicing—with respect to critical infrastructure across subsectors such as telecommunications, utilities, energy, and transportation, each as identified in an appendix to the regulations.” *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ Non-controlling covered investments include those that that afford a foreign person certain access, rights, or involvement in certain types of U.S. businesses. *Id.* at 2.

whether there is a genuine national security risk and, if so, the extent of the risk.⁸⁶ If CFIUS finds a national security risk, a company may be able to mitigate such risk.⁸⁷ However, if the security risk cannot be mitigated, the foreign company would be prohibited from purchasing or investing in the American company.⁸⁸ If, after review, CFIUS recommends suspension or prohibition of the transaction, it is then referred to the President for a final determination.⁸⁹ The President is then required to make two findings to act on the recommendation. First, the President must find that “there is credible evidence that leads the President to believe that the foreign interest exercising control might take action that threatens to impair the national security.”⁹⁰ Second, the President must find “that provisions of law, other than section 721 and [IEEPA], do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security.”⁹¹

In 2019, after bipartisan requests,⁹² CFIUS began investigating ByteDance’s one billion dollar acquisition of U.S. company, Musical.ly, which “was fully rebranded as TikTok in 2018.”⁹³ Although the acquisition was completed two years before the review

⁸⁶ Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74,567, 74,568 (Dec. 8, 2008); LATHAM & WATKINS LLP, *supra* note 77, at 2.

⁸⁷ LATHAM & WATKINS LLP, *supra* note 77, at 6.

⁸⁸ *Id.*

⁸⁹ Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74,567, 74,569 (Dec. 8, 2008).

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² See Press Release, Chuck Schumer, Senate Minority Leader & Tom Cotton, Senator, Request Assessment of National Security Risks Posed by China-Owned Video-Sharing Platform, TikTok, A Potential Counterintelligence Threat With Over 110 Million Downloads in U.S., Alone (Oct. 24, 2019), <https://www.democrats.senate.gov/newsroom/press-releases/leader-schumer-senator-cotton-request-assessment-of-national-security-risks-posed-by-china-owned-video-sharing-platform-tiktok-a-potential-counterintelligence-threat-with-over-110-million-downloads-in-us-alone> [https://perma.cc/HLD3-3LSY].

⁹³ Haley Samsel, *U.S. Government Opens Official National Security Investigation Into TikTok*, SEC. TODAY (Nov. 4, 2019), <https://securitytoday.com/articles/2019/11/04/tiktok-national-security-investigation.aspx> [https://perma.cc/VV4R-PH5Q].

began, TikTok did not notify CFIUS when it acquired Musical.ly, which is why CFIUS could retrospectively investigate the deal.⁹⁴ TikTok claims it tried to cooperate with CFIUS once the investigation was opened.⁹⁵ Nevertheless, according to TikTok, “CFIUS never articulated any reason why TikTok’s security measures were inadequate to address any national security concerns,”⁹⁶ and “[d]espite these repeated efforts and concrete proposals to alleviate any national security concerns, the agency record reflects that CFIUS repeatedly refused to engage with ByteDance and its counsel about CFIUS’s concerns.”⁹⁷ TikTok noted that just minutes before midnight on the final day of the statutory review period, “the Committee issued a letter stating that ‘CFIUS has identified national security risks arising from the Transaction and that it has not identified mitigation measures that would address those risks.’”⁹⁸

In exercising executive power under IEEPA, President Trump relied on CFIUS’ conclusion to issue an additional Executive Order requiring ByteDance to sell TikTok and that it do so under CFIUS’ conditions.⁹⁹ Using CFIUS in this way is an extraordinary move because CFIUS reviews typically concern industries directly related to national security, such as infrastructure or telecommunications, not consumer tech companies like TikTok.¹⁰⁰ In 2019 alone, CFIUS conducted a review of 231 covered transactions and further

⁹⁴ Greg Roumeliotis, et al., *Exclusive: U.S. Opens National Security Investigation into TikTok – Sources*, REUTERS (Nov. 1, 2019, 11:21 AM) <https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL> [<https://perma.cc/RDY2-G86Z>].

⁹⁵ Complaint, *supra* note 6, at 14.

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.* at 15.

⁹⁹ Exec. Order Regarding the Acquisition of Musical.ly by Byte Dance Ltd., 85 Fed. Reg. 51,297, 51,297–98 (Aug. 14, 2020).

¹⁰⁰ Martin Chorzenpa, *The TikTok Deal is a Defining Moment for CFIUS*, BARRON’S (Sept. 17, 2020, 9:54 AM), <https://www.barrons.com/articles/the-tiktok-deal-is-a-defining-moment-for-cfius-51600350898> [<https://perma.cc/F33U-KWTN>].

investigated 113.¹⁰¹ A review of historical data concerning CFIUS reviews reveals that in 2019, CFIUS scrutinized deals at a rate of five times more than in the previous decade.¹⁰² In short, one thing should be clear to international tech companies about CFIUS: “[the] committee considers personal data a serious national security issue. It can and will block or unwind tech deals that give foreign access to Americans’ personal information.”¹⁰³

C. Entity List

A third possible executive branch route for banning TikTok is the U.S. Department of Commerce’s Entity List or the “blacklist of foreign companies.”¹⁰⁴ The Entity List is “a regulatory tool administered by the Commerce Department to protect U.S. national security and foreign-policy interests by restricting U.S. exports to a listed entity.”¹⁰⁵ Companies on the entity list are restricted from receiving certain exports that were manufactured or designed in the United States.¹⁰⁶ After being placed on the list, the Export Administration Regulations “impose[] additional license requirements on, and limits the availability of most license exceptions for exports, reexports, and transfers (in-country) to, listed entities.”¹⁰⁷ The license required to export to the entity is

¹⁰¹ COMM. ON FOREIGN INVEST. IN THE U.S., ANNUAL REPORT TO CONGRESS 2 (2019), <https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf> [<https://perma.cc/5LX5-8XAS>].

¹⁰² Chorzempa, *supra* note 100.

¹⁰³ Dan Mogin & Jennifer M. Oliver, *POTUS Uses CFIUS to Unwind TikTok Deal, Fears Chinese Government Will Get Americans’ Private Data*, NAT’L L. REV. (Aug. 18, 2020), <https://www.natlawreview.com/article/potus-uses-cfius-to-unwind-tiktok-deal-fears-chinese-government-will-get-americans> [<https://perma.cc/XAQ6-ZCDT>].

¹⁰⁴ Leskin, *supra* note 20.

¹⁰⁵ Beau Barnes, et al., *Trump Can’t Ban TikTok but He Can Hurt It*, FOREIGN POL’Y (July 24, 2020, 5:01 PM), <https://foreignpolicy.com/2020/07/24/trump-cant-ban-tiktok-free-chinese-apps/> [<https://perma.cc/MY3Q-KJW8>].

¹⁰⁶ Mengqi Sun, *U.S. Increasingly Uses Trade Blacklist for Foreign Policy Goals*, WALL ST. J. (Aug. 31, 2020, 6:22 PM), <https://www.wsj.com/articles/u-s-increasingly-uses-trade-blacklist-for-foreign-policy-goals-11598912568?mod=searchresults&page=2&pos=7> [<https://perma.cc/UXB2-CMCC>].

¹⁰⁷ Addition of Entities to the Entity List, 84 Fed. Reg. 22,961, 22,961 (May 21, 2019) (to be codified at 15 C.F.R. pt. 744).

subject to review with a presumption of denial.¹⁰⁸ Therefore, once placed on the list, it is challenging for foreign companies to receive any U.S. exports. Multiple Chinese tech companies are already on the list, including Huawei and many of its affiliates.¹⁰⁹

For example, the Commerce Department added Huawei to the list in May of 2019 because it determined that Huawei was engaging in practices that undermined national security and foreign policy interests of the United States.¹¹⁰ The main consequence of the placement of Huawei on the list is that they will not be able to purchase semiconductors, including chips that are the essential components of mobile phones, that have been developed or created with U.S. software or technology.¹¹¹ Before being placed on the Entity List, Huawei and its chief financial officer were indicted by the U.S. Department of Justice for various fraud crimes and IEEPA violations because they had supplied Iran with American goods in violation of trade sanctions.¹¹² Further, the U.S. government's concerns center on how intertwined Huawei is with the Chinese government.¹¹³ For example, the Central Intelligence Agency (“CIA”) flagged that Huawei receives funding from China's

¹⁰⁸ *Id.*

¹⁰⁹ David Shepardson & Karen Freifeld, *China's Huawei, 70 Affiliates Placed on U.S. Trade Blacklist*, REUTERS (May 15, 2019, 6:14 PM), <https://www.reuters.com/article/us-usa-china-huaweitech/chinas-huawei-70-affiliates-placed-on-us-trade-blacklist-idUSKCN1SL2W4> [<https://perma.cc/LZ37-4AAN>].

¹¹⁰ 15 C.F.R. § 744 (2019) (illustrating that Huawei has been indicted in the U.S. District Court for the Eastern District of New York on violations of the IEEPA “by . . . causing the export, reexport, sale and supply, directly and indirectly, of goods, technology and services (banking and other financial services) from the United States to Iran and the government of Iran without obtaining a license”).

¹¹¹ David Shepardson, *U.S. Tightening Restrictions on Huawei Access to Technology, Chips*, REUTERS (Aug. 17, 2020, 7:33 AM) <https://www.reuters.com/article/us-usa-huawei-tech/u-s-tightening-restrictions-on-huawei-access-to-technology-chips-idUSKCN25D1CC> [<https://perma.cc/4SQ3-N8VU>].

¹¹² Superseding Indictment at 10–19, *United States v. Huawei Tech. Co.*, Cr. No. 18-457 (S-2) (AMD) (2019), <https://www.justice.gov/opa/press-release/file/1125021/download> [<https://perma.cc/5SXS-R8AQ>].

¹¹³ Steven Musil, *CIA Reportedly Says Huawei Funded by Chinese State Security*, CNET (Apr. 21, 2019, 8:25 AM PT), <https://www.cnet.com/news/cia-reportedly-says-huawei-funded-by-chinese-state-security/> [<https://perma.cc/UZ2P-GGTX>].

National Security Commission, the People’s Liberation Army, and another unnamed part of the Chinese state intelligence network.¹¹⁴ The placement of Huawei on the list is primarily due to the perceived risk that Huawei would grant Chinese authorities access to sensitive American user data.¹¹⁵

Before the Trump Administration, the Entity List had been “used to target violations of U.S. export control or economic sanctions laws, but in recent years, the scope of ‘national security’ has expanded.”¹¹⁶ Therefore, “[i]t would not be a stretch for the United States to pronounce that ByteDance’s access to the personal data of U.S. citizens threatens U.S. national security interests,”¹¹⁷ which is exactly what Trump did in his first Executive Order concerning TikTok.¹¹⁸

Overall, the current legal framework is adequate to allow the executive branch to regulate and ban any foreign company it deems a national security risk. Companies must be wary of this when conducting their business with the U.S. and be aware of the consequences of being deemed a “national security threat.” Additionally, although deference to national security concerns may be appropriate, it must be ensured that those concerns are legitimate and not just perceived. In sum, the United States is serious about protecting American data and privacy from peering foreign eyes and is not afraid to take dramatic steps to protect that interest.

III. IMPLICATIONS OF A BAN ON FIRST AMENDMENT RIGHTS

Although there are multiple methods the executive branch can use to attempt to “ban” TikTok, these methods may not pass constitutional muster because they potentially implicate First Amendment freedoms.¹¹⁹ Cyberspace and social media, in particular, have become the “quintessential forum for the exercise of First Amendment right[s].”¹²⁰ However, the Supreme Court has

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ Barnes, et al., *supra* note 105.

¹¹⁷ *Id.*

¹¹⁸ Exec. Order No. 13942, *supra* note 11.

¹¹⁹ *Id.*

¹²⁰ *Packingham v. North Carolina*, 137 S.Ct. 1730, 1735 (2017).

not directly addressed how governmental regulation of modern social media fits into the First Amendment framework.¹²¹ Here, First Amendment questions arise because TikTok is a “widely-used platform for U.S. entities and individuals to engage in self-expression—including political expression—and to share original content.”¹²² Other IEEPA bans have not targeted any other company similarly engaged in free expression.¹²³ In the litigation surrounding the ban, TikTok claimed that it has First Amendment protections via the rights of creators on TikTok, and in TikTok’s source code or software, while the U.S. government countered that there is no First Amendment implication at all.¹²⁴ This section addresses the First Amendment rights of content creators, platform owners’ rights in their source code, and whether national security sufficiently outweighs those rights.

A. First Amendment Rights of TikTok Content Creators and Users

Although the Supreme Court has not explicitly addressed the medium of social media in the context of the First Amendment, it is likely that content creators¹²⁵ have First Amendment protections in the content they create, so long as that content would not be exempt from protection under a separate First Amendment doctrine, such as obscenity.¹²⁶ Concurring in *Kovacs v. Cooper*,¹²⁷ Justice Jackson wrote, “[t]he moving picture screen, the radio, the newspaper, the handbill, the sound truck and the street corner orator have differing natures, values, abuses and dangers. Each, in my view, is a law unto

¹²¹ VALERIE C. BRANNON, CONG. RSCH. SERV., R45650, FREE SPEECH AND THE REGULATION OF SOCIAL MEDIA CONTENT 40 (Mar. 27, 2019), <https://fas.org/sgp/crs/misc/R45650.pdf> [<https://perma.cc/53P7-VN93>].

¹²² Elena Chachko, *Could the TikTok and WeChat Executive Orders Undermine IEEPA?*, LAWFARE (Aug. 8, 2020, 2:49 PM), <https://www.lawfareblog.com/could-tiktok-and-wechat-executive-orders-undermine-ieepa> [<https://perma.cc/WST5-T4HJ>].

¹²³ *Id.*

¹²⁴ Defendant’s Memorandum, *supra* note 56, at 29.

¹²⁵ TikTok itself is a content creator. The company’s account, @tiktok, creates posts that relate to topics and interests that the company cares about. Supplemental Declaration of Vanessa Papas at 2, *TikTok Inc. v. Trump*, No. 1:20-cv-02658 (2020).

¹²⁶ See *Miller v. California*, 413 U.S. 15, 23 (1973).

¹²⁷ *Kovacs v. Cooper*, 336 U.S. 77, 77 (1949).

itself.”¹²⁸ The same is certainly true about social media, and application of the First Amendment will account for the uniqueness of the medium. Social media is unique, compared to other more traditional mediums of expression, because of the immediacy of posting, interactivity among users, and broad accessibility, all without the editorial filters to which traditional media, such as newspapers and broadcast journalism, are subject.¹²⁹

1. Content-Based Restrictions

Assuming that content creation on TikTok falls within speech that is protected by the First Amendment, the next determination is whether such a ban is content-based or content-neutral. If a regulation of speech is content-based,¹³⁰ the Court must balance constitutional interests and the regulatory interests against strict scrutiny.¹³¹ The higher the value of the speech, the stronger the constitutional interest is.¹³² Many consider pure political speech as the most high-valued form of speech, and any regulation of it would be subject to strict scrutiny.¹³³ Strict scrutiny requires the government to prove that the proposed ban is “narrowly tailored to promote a compelling Government interest.”¹³⁴ Here, the compelling government interest is protecting national security.¹³⁵

Content-based restrictions are also subject to prior restraint analysis.¹³⁶ A prior restraint “is a restriction on speech that is imposed prior to the dissemination of a communication.”¹³⁷ The Supreme Court has expressed that “[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption

¹²⁸ *Id.* at 97 (Jackson, J., concurring) (1949).

¹²⁹ RUSSELL L. WEAVER, UNDERSTANDING THE FIRST AMENDMENT 320 (7th ed. 2020).

¹³⁰ A regulation is content based if it is regulating because of the message or idea being communicated. *Id.* at 36.

¹³¹ *See* Reed v. Town of Gilbert, 576 U.S. 155, 165 (2015).

¹³² WEAVER, *supra* note 129 at 13–14, 36.

¹³³ *Id.*; Kusper v. Pontikes, 414 U.S. 51, 56–57 (1973).

¹³⁴ United States v. Playboy Ent. Grp., Inc., 529 U.S. 803, 813 (2000).

¹³⁵ Exec. Order No. 13942, *supra* note 11.

¹³⁶ DVD Copy Control Ass’n, Inc. v. Bunner, 75 P.3d 1, 17 (Cal. 2003).

¹³⁷ WEAVER, *supra* note 129 at 118.

against its constitutional validity.”¹³⁸ Therefore, the government “carries a heavy burden of showing justification for the imposition of such a restraint.”¹³⁹ There is a small exception for expression that causes an immediate threat to national security.¹⁴⁰ However, the burden is still on the government to prove that national security is threatened.¹⁴¹

TikTok and its users believe the ban is a content-based restriction and a prior restraint because the platform is used for political speech¹⁴² and disseminating pro-Chinese government content,¹⁴³ which was contrary to the Trump Administration’s goals.¹⁴⁴ The U.S. District Court for the Eastern District of Pennsylvania did not find this argument persuasive in evaluating the first round of prohibitions on TikTok because “pre-existing users” of TikTok¹⁴⁵ “will continue to be able to share their content and communicate on the application,” despite TikTok’s impending removal from app stores.¹⁴⁶ The court also found that the prohibition

¹³⁸ *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963). *See also* *Near v. Minnesota*, 283 U.S. 697, 716 (1931).

¹³⁹ *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971).

¹⁴⁰ *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 716 (1931) (explaining the kind of “exceptional cases” where prior restraints would be allowed to protect national security including, for example, “obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops”).

¹⁴¹ *Id.*

¹⁴² Brief for Jeffrey A. Lovitky, as Amicus Curiae Supporting Plaintiffs at 6–7, *TikTok v. Trump*, Case No. 20-cv-2658 (2020) (explaining how TikTok is used to disseminate political speech).

¹⁴³ Executive Order 13942 claims that “TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China’s treatment of Uyghurs and other Muslim minorities.” Exec. Order No. 13942, *supra* note 11. This mobile application may also be used for disinformation campaigns that benefit the Chinese Communist Party, such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus.” *Id.*

¹⁴⁴ Brief for Jeffrey A. Lovitky, *supra* note 142, at 2.

¹⁴⁵ “Pre-existing users” refers to those who downloaded TikTok before the September 27th prohibition from the app store took place.

¹⁴⁶ *Marland v. Trump*, 2020 U.S. Dist. LEXIS 177129, 2020 WL 5749928 at *15 (E.D. Pa. 2020).

on TikTok made “no distinction between favored and disfavored content,” therefore, the ban is not a content-based restriction.¹⁴⁷

However, the Eastern District of Pennsylvania left the question open about whether the later impending restrictions on TikTok would be in line with the requirements of the First Amendment because of the Northern District of California’s decision in *U.S. WeChat Users All. v. Trump*.¹⁴⁸ In that case, a group of WeChat users successfully moved for an injunction to halt an Executive Order which would also effectively ban WeChat in the United States. Chinese tech company Tencent owns WeChat and originally began as a messaging service but has transformed into a “super app” with integrated games, banking, ride-hailing, and meal delivery services.¹⁴⁹ WeChat is the predominant social media app in China because the Chinese government blocks western apps like Facebook.¹⁵⁰ The Northern District of California decided that the WeChat users would likely succeed on the merits of their First Amendment challenge to an outright ban of WeChat. The court came to this conclusion because “evidence demonstrated that ‘WeChat is effectively the only means of communication for many’ in the Chinese-speaking and Chinese-American community, and ‘there are no viable substitute platforms or apps’” to communicate with those located in China.¹⁵¹ In comparison, TikTok is not used as the sole line of communication among people in different countries, and there is a multitude of other apps available that provide similar functions.¹⁵²

¹⁴⁷ *Id.*

¹⁴⁸ *U.S. WeChat Users All. v. Trump*, No. 20-cv-05910-LB, 2020 WL 5592848 (N.D. Cal. 2020).

¹⁴⁹ Arjun Kharpal, *Everything You Need to Know About WeChat – China’s Billion-User Messaging App*, CNBC (Feb. 4, 2019, 2:22 AM), <https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html> [<https://perma.cc/9YCT-8RPD>].

¹⁵⁰ *Id.*

¹⁵¹ Marland, 2020 WL 5749928 at *15 (citing *U.S. WeChat Users All. v. Trump*, 2020 WL 5592848 (N.D. Cal. 2020)).

¹⁵² Jefferson Graham, *TikTok Ban: Here are 5 Cool Alternatives*, USA TODAY (Sept. 19, 2020, 9:31 PM), <https://www.usatoday.com/story/tech/2020/09/18/tiktok-ban-alternatives-triller-instagram-reels-byte-dubsmash-youtube/5824856002/> [<https://perma.cc/225V-BKZE>].

2. *Content-Neutral Restrictions*

An outright ban of TikTok appears to be content-neutral rather than content-based and would have to pass only intermediate scrutiny compared to the more stringent strict scrutiny review.¹⁵³ “A content-neutral, time-place-or-manner restriction survives intermediate scrutiny if it (1) is narrowly tailored, (2) serves a significant government interest unrelated to the content of the speech, and (3) leaves open adequate channels for communication.”¹⁵⁴ Protecting national security is a significant government interest, and banning TikTok arguably would leave open other adequate channels for communication given the vast number of social media apps available, some of which have rolled out features similar to TikTok’s.¹⁵⁵ Whether a complete ban is narrowly tailored poses a different question and turns directly upon how exactly TikTok threatens national security.

B. First Amendment Rights of Platform Owners in their Source Code

TikTok is a mobile software app, and the underlying code could be covered as speech under the First Amendment.¹⁵⁶ Although the Supreme Court has not yet addressed whether the First Amendment protects software, the Northern District of California has held that “[I]ike music and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who can read it.”¹⁵⁷ Therefore, the First Amendment covers software. Additionally, the Sixth Circuit held

¹⁵³ See also *U.S. WeChat Users All. v. Trump*, No. 20-cv-05910-LB, 2020 WL 5592848 at *10 (N.D. Cal. 2020).

¹⁵⁴ *Id.*

¹⁵⁵ Jason Aten, *Instagram Reels Copies TikTok, and Is an Example of Everything Wrong With Facebook*, INC. (Aug. 6, 2020), <https://www.inc.com/jason-aten/instagram-reels-is-a-copy-of-tiktok-an-example-of-everything-wrong-with-facebook.html> [<https://perma.cc/4HK2-BCZZ>].

¹⁵⁶ Complaint, *supra* note 6, at 2.

¹⁵⁷ See *Bernstein v. U.S. Dep’t of State*, 922 F. Supp. 1426, 1435–36 (N.D. Cal. 1996). See also *Green v. U.S. Dep’t of Just.*, 392 F. Supp. 3d 68, 86 (D.D.C. 2019). However, *Bernstein* dealt with a plaintiff professor who wished to distribute the source code in order for people to see how computers work. In contrast, TikTok, at the time of the first Executive Order, did not make their source code easily accessible. Defendant’s Memorandum, *supra* note 56, 31.

that “because computer source code is an expressive means for the exchange of information and ideas about computer programming, it is protected by the First Amendment.”¹⁵⁸

In order for TikTok’s software to receive First Amendment protections, TikTok would need to establish that its code “possesses sufficient communicative elements to bring the First Amendment into play.”¹⁵⁹ There must be “[a]n intent to convey a particularized message . . . and in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it.”¹⁶⁰ The issue with source code is that not every human will be able to understand it because the average person is not versed in computer programming languages. However, treating source code as its own language, such as English or Spanish, could remedy this problem.¹⁶¹ A Second Circuit opinion echoed and expanded this line of thinking when it upheld First Amendment protections for computer code that “convey[s] information capable of comprehension and assessment by a human being”; however, the court determined First Amendment protections would not apply when “a human’s mental faculties do not intercede in executing the instructions.”¹⁶²

In the modern digital age, the First Amendment should apply to software and the apps it powers. Although TikTok filed its lawsuit in the Central District of California,¹⁶³ the Central District will likely find the Northern District of California’s holding, that software is covered by the First Amendment,¹⁶⁴ persuasive. This case, and the existence of previously mentioned contrary precedent, could then set the stage for Ninth Circuit review and possibly even review by

¹⁵⁸ See *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000).

¹⁵⁹ *Texas v. Johnson*, 491 U.S. 397, 404 (1989).

¹⁶⁰ *Spence v. Washington*, 418 U.S. 405, 410–11 (1974).

¹⁶¹ Jorge R. Roig, *Decoding First Amendment Coverage of Computer Source Code in the Age of Youtube, Facebook, and the Arab Spring*, 68 N.Y.U. ANN. SURV. OF AM. L., 319, 327 (2013), https://www.law.nyu.edu/sites/default/files/upload_documents/NYU-Annual-Survey-68-2-Roig.pdf [<https://perma.cc/HMK8-MGPH>].

¹⁶² *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 448 n.20 (2d Cir. 2001).

¹⁶³ Complaint, *supra* note 6, at 2.

¹⁶⁴ See *Bernstein v. U.S. Dep’t of State*, 922 F. Supp. 1426, 1435–36 (N.D. Cal. 1996). See also *Green v. U.S. Dep’t of Just.*, 392 F. Supp. 3d 68, 86 (D.D.C. 2019).

the Supreme Court given the high-profile nature of the case and the national issues at stake.¹⁶⁵ Even if software code is determined to be protected speech under the First Amendment, the question of what balance between freedom of speech and national security concerns remains.

C. Balancing the First Amendment and National Security

Although the Supreme Court has not directly dealt with balancing the First Amendment and national security in the context of a social media app, it is important to consider judicial deference to the executive branch when national security is at stake.¹⁶⁶ In the past, the Supreme Court has been incredibly deferential to the executive branch citing national security concerns.¹⁶⁷ For example, in *Trump v. Hawaii*,¹⁶⁸ the President had issued an Executive Order restricting entry to the United States by individuals from eight

¹⁶⁵ In response to TikTok’s arguments for First Amendment protection, the Trump Administration countered that it is not regulating speech at all, but is instead regulating business transactions through economic regulation. Defendant’s Memorandum, *supra* note 56, at 29. First, they argued that there generally is no First Amendment protection concerning such transactions. *Id.* Second, because the restrictions imposed by the Trump Administration are “across-the-board” and “justified by weighty concerns of foreign policy,” there is no First Amendment protection. *Id.* (quoting *Regan v. Wald*, 468 U.S. 222, 241–42 (1984)). Third, the D.C. Circuit has also held, in the context of common carriers, that “such entities . . . merely facilitate the transmission of the speech of others rather than engage in speech in their own right,” therefore, the First Amendment does not apply to simply hosting a platform. *Id.* (quoting *U.S. Telecom Ass’n v. FCC*, 825 F.3d 674, 741 (D.C. Cir. 2016)). For example, telecommunications common carriers are similar to mobile apps in that they provide a platform and nothing more. Therefore, the D.C. Circuit opinion would most likely cover mobile apps in the same way it covers common carriers. *Id.*

¹⁶⁶ Bree Evans, *The National Security Exception to the First Amendment Prohibition on Prior Restraints*, AM. UNIV. NAT’L SEC. L. BRIEF (Apr. 10, 2020, 6:41 PM), <https://nationalsecuritylawbrief.com/2020/04/10/the-national-security-exception-to-the-first-amendment-prohibition-on-prior-restraints> [https://perma.cc/9USF-YLDS].

¹⁶⁷ See *Korematsu v. U.S.*, 323 U.S. 214, 217–18 (1944) (holding that it was within the war power of Congress and the executive to exclude those of Japanese ancestry from the West Coast because exclusion had a “definite and close relationship to the prevention of espionage and sabotage”); *Trump v. Hawaii*, 138 S. Ct. 2392, 2392 (2018).

¹⁶⁸ *Trump*, 138 S. Ct. at 2392.

countries that might pose a national security threat.¹⁶⁹ The Supreme Court held that “when the President adopts ‘a preventive measure . . . in the context of international affairs and national security,’ he is ‘not required to conclusively link all of the pieces in the puzzle before [courts] grant weight to [his] empirical conclusions.’”¹⁷⁰ In a rebuke of judicial review of the issue, the Court also held that when “matters may implicate ‘relations with foreign powers,’ . . . such judgments ‘are frequently of a character more appropriate to either the Legislature or the Executive.’”¹⁷¹ Continuing on this note, the Court wrote that “[j]udicial inquiry into the national-security realm raises concerns for the separation of powers’ by intruding on the President’s constitutional responsibilities in the area of foreign affairs.”¹⁷² And if the point was not already clear, the Court explicitly stated, “[a]ny rule of constitutional law that would inhibit the flexibility’ of the President ‘to respond to changing world conditions should be adopted only with the greatest caution,’ and our inquiry into matters of . . . national security is highly constrained.”¹⁷³

However, the threat to national security must be legitimate and not merely perceived.¹⁷⁴ The Supreme Court made this clear in *New York Times Co. v. United States*¹⁷⁵ when the Court held that the government had not met its burden for imposing a prior restraint when it sought to enjoin the publication of classified material relating to the Vietnam War.¹⁷⁶ In his concurrence, Justice Brennan highlighted that First Amendment jurisprudence does not allow prior restraints “predicated upon surmise or conjecture that

¹⁶⁹ *Id.* at 2399.

¹⁷⁰ *Id.* at 2409 (quoting *Holder v. Humanitarian L. Project*, 561 U.S. 1, 35 (2010)).

¹⁷¹ *Id.*

¹⁷² *Id.* at 2419 (quoting *Ziglar v. Abbasi*, 137 S. Ct. 1843 (2017)).

¹⁷³ *Id.* at 2419–20 (quoting *Matthews v. Diaz*, 426 U.S. 67, 81–82 (1976)).

¹⁷⁴ Ojan Aryanfard, *National Security*, THE FIRST AMENDMENT ENCYCLOPEDIA, [https://www.mtsu.edu/first-amendment/article/1134/national-security#:~:text=the%20Associated%20Press\)-,Despite%20the%20absolute%20language%20of%20the%20First%20Amendment%2C%20wars%2C%20threats,Amendment%20freedoms%20throughout%20U.S.%20history](https://www.mtsu.edu/first-amendment/article/1134/national-security#:~:text=the%20Associated%20Press)-,Despite%20the%20absolute%20language%20of%20the%20First%20Amendment%2C%20wars%2C%20threats,Amendment%20freedoms%20throughout%20U.S.%20history) [https://perma.cc/YUS7-YAZN] (last visited Jan. 16, 2021).

¹⁷⁵ *N.Y. Times Co. v. United States*, 403 U.S. 713, 713 (1971).

¹⁷⁶ *Id.* at 714.

untoward consequences may result.”¹⁷⁷ Justice Brennan further explained that for the national security exception to apply, there must be both “governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea.”¹⁷⁸

TikTok’s situation is different from the New York Times because the New York Times itself wished to release information it had obtained, and the government contended the publication was a threat to national security.¹⁷⁹ In contrast, the national security concern surrounding TikTok is that Chinese ownership may lead to improper use of American data for espionage purposes because of the structure of Chinese law.¹⁸⁰ The thrust of the government’s national security concerns do not concern posts on TikTok, but rather data collection and content moderation practices.¹⁸¹

Because of the substantial deference towards executive action, particularly in the context of national security, it is doubtful that a court will find that freedom of expression on TikTok, or any other similarly situated app, outweighs *legitimate* national security concerns, mainly because it is unclear whether the content-based restriction framework would even protect such speech. Likely, a TikTok ban will not be considered a content-based restriction because the entire platform would be restricted for reasons other than the content that is posted on the platform. Therefore, such a content-neutral ban would not be subject to prior restraint analysis. However, even if a court determined that the ban was content-based and subject to prior restraint analysis, the government could still ban the app so long as the government alleges and proves that the app will inevitably, directly and immediately cause harm to national security.¹⁸²

¹⁷⁷ *Id.* at 725–26 (Brennan, J., concurring).

¹⁷⁸ *Id.* at 726–27.

¹⁷⁹ *Id.* at 714.

¹⁸⁰ Jordan Schneider, *The U.S. Is Right to Worry About TikTok*, LAWFARE (Aug. 3, 2020, 2:58 PM), <https://www.lawfareblog.com/us-right-worry-about-tiktok> [<https://perma.cc/9ZCQ-6FY9>].

¹⁸¹ *Id.*

¹⁸² See discussion *supra* p. 29.

1. *TikTok Ban as a Content-Neutral Restriction*

Analyzing a TikTok ban as a content-neutral restriction also leads to the conclusion that it is likely permissible under the First Amendment if the government can show that banning TikTok is the narrowest approach for achieving the significant government interest of protecting national security. The Supreme Court has been increasingly deferential to the executive branch in national security matters, as can be seen in the shift of the Court's rhetoric from the *New York Times v. United States* decision to the *Trump v. Hawaii* decision.¹⁸³ It appears the Court may even be backing away from its steep requirement of the government to show in definite terms how national security is implicated. Instead, the court could defer to executive empirical conclusions concerning issues of national security, much like the Court's approach in *Trump v. Hawaii*, in order to allow the Executive Branch flexibility in adapting to modern challenges. Under this deferential approach, the government would only need some piece of evidence to support such a conclusion and will not have to "link all the pieces of the puzzle" before acting.¹⁸⁴ Such deference on national security matters and the wide availability of U.S.-owned social media apps, which leave open other adequate channels of communication, should concern foreign social media app owners. This concern is heightened for Chinese owners or other countries that the U.S. government treats similarly to China. Social media app owners should be wary of being perceived as a national security threat in order to continue to operate in the United States.¹⁸⁵

¹⁸³ See discussion *supra* pp. 28–30.

¹⁸⁴ *Trump v. Hawaii*, 138 S.Ct. 2392, 2409 (2018).

¹⁸⁵ In *U.S. WeChat Users Alliance v. Trump*, the Northern District of California issued a preliminary injunction halting the WeChat ban because the Plaintiffs had presented serious questions of whether the ban would constitute a prior restraint on their communication. *U.S. WeChat Users All. v. Trump*, No. 20-CV-05910-LB, 2020 WL 5592848, at *10 (N.D. Cal. 2020). This argument turned on the fact that WeChat is the main avenue of communication for members of the Chinese-speaking and Chinese-American community. *Id.* Additionally, it is one of the only ways that Chinese-Americans can communicate with family and friends in China. *Id.* This is because China has banned citizens from accessing the majority of American social media apps. *Id.* This is different from TikTok because other

2. *Applying the Terrorism Approach to Cyber-Espionage*

Another argument to consider regarding the First Amendment and national security could be comparing cyber-espionage and foreign terrorism. Although the government did not consider this argument in its reply brief, it could favor the government because courts have previously held that national security concerns outweigh foreign terrorists' First Amendment rights and access to social media platforms.¹⁸⁶ Terror organizations have previously taken advantage of social media apps in order to spread their messages and recruit new supporters.¹⁸⁷ This activity draws parallels to allegations that the Chinese government uses social media platforms to recruit Chinese-Americans and former intelligence community members to conduct espionage against the United States on China's behalf.¹⁸⁸ This is important considering that one national security concern cited by the Congressional lawmakers regarding TikTok was that its data collection practices would allow the Chinese government the opportunity to build dossiers on millions of U.S. citizens.¹⁸⁹ These

social media apps, such as Instagram and Facebook, can step in as a similar platform that provides similar functions.

¹⁸⁶ See *Holder v. Humanitarian L. Project*, 130 S. Ct. 2705, 2711 (2010).

¹⁸⁷ Jaelyn K. Haughom, *Combating Terrorism in a Digital Age: First Amendment Implications*, FREEDOM F. INST., (Nov. 16, 2016), <https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combating-terrorism-in-a-digital-age-first-amendment-implications/> [<https://perma.cc/622A-37RX>].

¹⁸⁸ Edward Wong, *How China Uses LinkedIn to Recruit Spies Abroad*, N.Y. TIMES (Sept. 27, 2019), <https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html> [<https://perma.cc/54C6-734J>]. See *The Nevernight Connection*, FBI, <https://www.fbi.gov/investigate/counterintelligence/the-china-threat/clearance-holders-targeted-on-social-media-nevernight-connection> [<https://perma.cc/CLJ2-UQB7>] (last visited Oct. 21, 2020) (leading the FBI to create a warning film); Mike Giglio, *China's Spies Are On the Offensive*, ATLANTIC (Aug. 26, 2019), <https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/> [<https://perma.cc/W78E-5MEX>]. See Hammaad Salik & Zaheema Iqbal, *Social Media and National Security*, GEOPOLITICS (Sept. 9, 2019), <https://thegeopolitics.com/social-media-and-national-security/> [<https://perma.cc/B5XM-EADV>].

¹⁸⁹ This could occur “in a Cambridge Analytica-style fashion, that such information could be used to develop profiles on Americans in ways that lend themselves to enhanced microtargeting on social media and other platforms.” Sherman, *supra* note 60.

dossiers could aid in the Chinese government's recruitment of Americans for espionage purposes.¹⁹⁰

Although the executive branch likely has the power within the legal framework to ban TikTok, the First Amendment implications of completely banning a social media app may prove problematic. This issue leaves open many questions concerning how the strong government interests in national security interacts with the competing constitutional interest of the First Amendment, and the lack of case law on the subject may soon require courts to draw that line.

IV. TIKTOK AS AN EXAMPLE FOR OTHER FOREIGN TECH AND APP COMPANIES

As American and Chinese relations continue to deteriorate and global competition, foreign policy, and national security concerns become improperly conflated, it is more important now than ever for international tech and app companies to prepare for the global internet's splintering.¹⁹¹ The TikTok ban could "set[] a precedent for the government to ban other apps or even for other global apps to be inaccessible to the United States' market."¹⁹² Companies who wish to operate in both China and the United States may need to set up two completely different frameworks for operating their businesses in this new age of "net nationalism."¹⁹³

A country that engages in net nationalism "views the country's internet primarily as a tool of state power," where "economic growth, surveillance and thought control . . . are the internet's most important functions."¹⁹⁴ A classic example of what net nationalism could lead to is the Chinese government's "Great Firewall."¹⁹⁵ In

¹⁹⁰ *Id.*

¹⁹¹ Gertz, *supra* note 76.

¹⁹² Queenie Wong et al., *The TikTok saga: Everything you need to know*, CNET (Sept. 18, 2018, 7:11 AM), <https://www.cnet.com/news/trump-vs-tiktok-everything-you-need-to-know/> [<https://perma.cc/ZP8D-J6VU>].

¹⁹³ Wu, *supra* note 17.

¹⁹⁴ *Id.*

¹⁹⁵ Christopher Mims, *In a U.S.-China Tech Divorce, Businesses Would Have to Pick Sides*, WALL ST. J. (Aug. 15, 2020, 12:00 AM), <https://www.wsj.com/>

China, websites such as Facebook, Twitter, Netflix, YouTube, Wikipedia, and many other mainstream sites from the United States and Europe are banned.¹⁹⁶ Other countries have also engaged in similar practices, including Turkey, Iran, Saudi Arabia, and India.¹⁹⁷

A. The U.S. Clean Network Initiative and its Effects

Under the Trump Administration, the United States proposed its version of net nationalism, the “Clean Network.”¹⁹⁸ On a

articles/in-a-u-s-china-tech-divorce-businesses-would-have-to-pick-sides-11597464037?mod=searchresults&page=4&pos=19 [https://perma.cc/WN2L-SY5V].

¹⁹⁶ *Id.*

¹⁹⁷ *Id.* In India, whenever there are signs of civil unrest or disturbance, various levels of government shut the internet down. See Jeffrey Gettleman et al., *India Adopts the Tactic of Authoritarians: Shutting Down the Internet*, N.Y. TIMES, (Dec. 20, 2019) <https://www.nytimes.com/2019/12/17/world/asia/india-internet-modi-protests.html> [https://perma.cc/AK4A-HLKK]. In 2018 alone, the government cut internet service at least 134 times. *Id.* Iran has likewise used the tactic of shutting down the internet to cull protests and unrest. See Michael Safi, *Iran’s Digital Shutdown: Other Regimes ‘Will be Watching Closely,’* GUARDIAN, (Nov. 21, 2019, 13:07), <https://www.theguardian.com/world/2019/nov/21/irans-digital-shutdown-other-regimes-will-be-watching-closely> [https://perma.cc/AMH4-DYAV]. However, Iran has managed to cut its citizens access to global internet, while allowing a state-backed internal network to operate even during internet shutdowns. *Id.*

¹⁹⁸ See Press Statement, Michael R. Pompeo, Sec’y of State, Dep’t of State, Announcing the Expansion of the Clean Network to Safeguard America’s Assets (Aug. 5, 2020), <https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/> [https://perma.cc/7CWQ-X8TY]. The Clean Network was first envisioned following the Prague Proposals in May 2019. See Michael R. Pompeo, *Secretary Pompeo’s Video Remarks at the Prague 5G Security Conference 2020*, U.S. DEP’T OF STATE (Sept. 23, 2020), <https://2017-2021.state.gov/secretary-pompeos-video-remarks-at-the-prague-5g-security-conference-2020/index.html> [https://perma.cc/F9GS-9VGM]. At the Prague 5G Security Conference, representatives from over thirty countries, the European Unions, the North Atlantic Treaty Organization, and industry leaders, “participated in discussions regarding the important national security, economic, and commercial considerations that must be part of each country’s evaluation of 5G vendors.” *The Clean Network*, U.S. DEP’T OF STATE, <https://www.state.gov/the-clean-network/> [https://perma.cc/P2L7-D67A] (last visited Oct. 21, 2020). The Prague Proposals include four categories: (1) policy, (2) technology, (3) economy, and (4) security, privacy, and resilience. PRAGUE 5G SECURITY CONFERENCE, THE PRAGUE PROPOSALS: THE CHAIRMAN STATEMENT ON CYBER SECURITY OF COMMUNICATION NETWORKS IN A GLOBALLY DIGITALIZED WORLD

now-archived webpage, the U.S. Department of State's "Clean Network" is described as the "Trump Administration's comprehensive approach to guarding our citizens' privacy and our companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party ("CCP")."¹⁹⁹ The implementation of the Clean Network would have meant "no Chinese apps in U.S. app stores, no U.S. data stored on the Chinese cloud, and no U.S. apps on Chinese smartphones."²⁰⁰ How the government would have enforced the Clean Network is unclear;²⁰¹ however, the initiative highlighted a growing trend towards net nationalism.²⁰²

The Clean Network Initiative had six goals: Clean Carrier, Clean Store, Clean Apps, Clean Cloud, Clean Cable, and Clean Path, and they were all antagonistic to China.²⁰³ The Clean Carrier goal would have forbidden Chinese carriers from being connected to U.S. telecommunications networks, reasoning that if they provided international telecommunications services to and from the United States, these carriers would threaten U.S. national security.²⁰⁴ The Clean Store goal would have removed Chinese and other "untrusted" apps from mobile app stores due to the threat the apps pose to American privacy, virus proliferation, content censoring, and propaganda and disinformation spread.²⁰⁵ The Clean Apps goal intended to prevent "untrusted" Chinese phone manufacturers, such

3–5 (May 3, 2019). Highlights of these proposals include that policies governing 5G networks "should be guided by the principles of transparency and equitability, taking into account the global economy," and that "[s]tate-sponsored incentives, subsidies, or financing of 5G communication networks and service providers should respect principles of fairness, be commercially reasonable, conducted openly and transparently, based on open market competitive principles." *Id.* at 3–5.

¹⁹⁹ Press Statement, *supra* note 198.

²⁰⁰ *Id.*; James Vincent, *The White House's plan to purge Chinese tech from the internet is just bluster — for now*, THE VERGE (Aug. 6, 2020, 12:45 PM), <https://www.theverge.com/2020/8/6/21356948/us-clean-network-purge-chinese-tech-apps-app-store-us-internet> [<https://perma.cc/UM4X-CG7B>] (describing the proposed program as "the US internet as it currently stands, but minus a lot of Chinese tech").

²⁰¹ Vincent, *supra* note 200.

²⁰² Wu, *supra* note 17.

²⁰³ *The Clean Network*, *supra* note 198.

²⁰⁴ *Id.*

²⁰⁵ *Id.*

as Huawei, from making available or pre-installing “trusted” apps on their app store.²⁰⁶ The Clean Apps goal further called for “trusted” apps to remove themselves from “untrusted” Chinese app stores to protect the innovation and reputation of leading U.S. and foreign companies.²⁰⁷ The Clean Cloud would have “prevent[ed] U.S. citizens’ most sensitive personal information and [U.S.] businesses’ most valuable intellectual property . . . from being stored and processed on cloud-based systems accessible to [U.S.] foreign adversaries”²⁰⁸ The Clean Cable goal would have “ensure[d] the undersea cables connecting our country to the global internet are not subverted for intelligence gathering” by China and would “work with foreign partners to ensure that undersea cables around the world aren’t similarly subject to compromise.”²⁰⁹ Lastly, the Clean Path goal would have “require[d] a Clean Path for all 5G network traffic entering and exiting U.S. diplomatic facilities.”²¹⁰ The Clean Path would have forbidden the use of “any transmission, control, computing, or storage equipment from untrusted [information technology] vendors, such as Huawei and ZTE”²¹¹ Again, these companies and Chinese technologies were considered “untrusted” by the Trump Administration because of Chinese laws which require Chinese companies to “comply with directives of the Chinese Communist Party.”²¹²

Although China’s Great Firewall is the quintessential example of “net nationalism,” some commenters suggest that the formerly proposed U.S. “Clean Network” is better compared to Russia’s approach to internet sovereignty.²¹³ For instance, in Russia, “the government has been able to pass some laws in areas like data localization, mandating that data concerning Russian citizens is processed in Russia, but it doesn’t have the control or resources that

²⁰⁶ *Id.* This means Huawei would not have access to “trusted” U.S. apps.

²⁰⁷ *Id.*

²⁰⁸ *Id.* Companies that would be affected by this include Alibaba, Baidu, China Mobile, China Telecom, and Tencent.

²⁰⁹ *Id.*

²¹⁰ *Id.*

²¹¹ *Id.*

²¹² *Id.*

²¹³ Vincent, *supra* note 200.

China has to directly oversee and censor the web so extensively.”²¹⁴ Like the United States, the Russian government does not have the same extensive censoring power as the Chinese government, which is why the comparison of the Clean Network to Russian internet sovereignty is more accurate in describing the style of net nationalism.²¹⁵

By August 2020, the United States claimed that over thirty countries have already signed on to the “Clean Network”—including the United Kingdom, Czech Republic, Poland, Sweden, Estonia, Romania, Denmark, and Latvia—by choosing to allow trusted vendors in their 5G networks.²¹⁶ Examples of trusted vendors include Telefonica, Oracle, Cisco, Telstra, Verizon, NTT, Sprint, Jio, Telenor, Telia, AT&T, Rakuten, KDDI, T-Mobile, Taiwan Mobile, SK Telecom, Optus, and Bell.²¹⁷ The United States had begun a high-pressure campaign of encouraging countries to reject Huawei as their 5G provider.²¹⁸ For example, the U.S. Department of State released an op-ed encouraging Brazil to avoid Chinese “bullying” and join the Clean Network by banning Huawei.²¹⁹ The op-ed called Huawei the “backbone of China’s worldwide surveillance state” and also voiced concerns about China’s National Intelligence Law, which requires companies to “turn[] over private

²¹⁴ *Id.*

²¹⁵ *Id.*

²¹⁶ U.S. DEP’T OF STATE, *supra* note 203. *But see* Leng Shumei, *US Unilaterally Put Nations on Clean Network List: Source*, GLOB. TIMES (Sept. 9, 2020, 20:28), <https://www.globaltimes.cn/content/1200334.shtml> [<https://perma.cc/G2JY-S6WW>]. The Global Times, which is a state-run Chinese tabloid, claims that the U.S. unilaterally put nations on the Clean Network list as a trick to put pressure on other countries to join. *Id.*

²¹⁷ U.S. DEP’T OF STATE, *supra* note 203.

²¹⁸ Julian E. Barnes & Adam Satariano, *U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist*, N.Y. TIMES (Mar. 17, 2019), <https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html?auth=login-facebook> [<https://perma.cc/7W2V-K97M>].

²¹⁹ Keith Krach, *Brazil Can Join the Growing Clean Network by Banning Huawei*, U.S. DEP’T OF STATE (Aug. 19, 2020), <https://www.state.gov/Brazil-Can-Join-the-Growing-Clean-Network-by-Banning-Huawei/> [<https://perma.cc/ND2X-GDP7>].

citizen and business data to the Chinese government upon request.”²²⁰

B. Sanctions as an Alternative to the Clean Network

Even without the Clean Network, the United States could still achieve similar results through sanctions.²²¹ For example, the United Kingdom (“U.K.”) announced it would ban Huawei from its 5G network after mounting pressure from the Trump Administration.²²² The U.K.’s decision came after the United States placed Huawei on the Entity List, which would require “foreign manufacturers using American chipmaking equipment to get a license before being able to sell semiconductors to Huawei.”²²³ Because of the U.S. sanctions on Huawei, the U.K. National Cyber Security Centre launched a review of the role of Huawei in their 5G network shortly thereafter.²²⁴ The Centre concluded that because Huawei no longer had access to trusted American technology, the security risk would be too significant to continue to allow Huawei to have a presence in the U.K.’s 5G network.²²⁵

Despite the change in presidential administrations, the effects of the United States pushing towards some form of a “Clean Network” would be widely felt. The move would lead to mass disruption in the global tech industry “by leveraging the tools of international trade.”²²⁶ For example, Chinese companies would be banned from

²²⁰ *Id.*

²²¹ Jonathan D. Pollack, *There are No Winners in US-China Technology Divide*, BROOKINGS (Sept. 14, 2020), <https://www.brookings.edu/blog/order-from-chaos/2020/09/14/there-are-no-winners-in-us-china-technology-divide/> [<https://perma.cc/3NTJ-3Z7S>].

²²² Thomas Macaulay, *UK Bans Huawei from 5G Network, Citing Security Risks Triggered by US sanctions*, THE NEXT WEB (July 14, 2020, 15:40 UTC), <https://thenextweb.com/neural/2020/07/14/uk-bans-huawei-from-5g-network-citing-security-risks-triggered-by-us-sanctions/> [<https://perma.cc/8W23-JRAH>].

²²³ Arjun Kharpal, *UK to Phase Out Huawei Gear from 5G Networks in a Major Policy U-turn After U.S. Sanctions Reports Say*, CNBC (July 6, 2020, 4:01 AM), <https://www.cnbc.com/2020/07/06/huawei-uk-5g-gear-to-be-phased-out-of-networks-in-major-policy-u-turn.html> [<https://perma.cc/S2Y2-XAKH>]; see discussion *supra* pp. 18–20.

²²⁴ *Id.*

²²⁵ *Id.*

²²⁶ Vincent, *supra* note 200.

using American software, which could lead to “hampering their ability to sell devices in lucrative European markets.”²²⁷ Additionally, the Clean Store goal would likely lead to the sale of more Chinese Apps to American companies to stay operative.²²⁸ This probable outcome shows that a TikTok ban may serve as an early step in purging Chinese technology from the United States and other western markets.

C. Movement Toward a “Splinternet”

Implementing a “Clean Network,” or other similar program, would increase the global move toward a “Splinternet,” or fractured internet, where the availability of certain apps and websites depends upon geographic location.²²⁹ As more nations move towards net nationalism and the “Splinternet” becomes more of a reality, this shift will have large effects on international companies and how these companies do business. Such restrictive and differing measures could make doing business so complicated and burdensome that the world would launch into a technological dark age, where global connectivity would no longer be the norm. In effect, a “Splinternet” would force companies and countries to decide whether they want to be within the U.S. or the Chinese sphere of internet influence.

However, a closed internet could impact some countries’ participation in the global economy, which relies on an open internet.²³⁰ Tim Wu, the law professor that coined the term “net

²²⁷ *Id.*

²²⁸ David X. Martin, *The Impact of the Clean Network Initiative on American Companies*, BRINK (Aug. 26, 2020), <https://www.brinknews.com/the-impact-of-the-clean-network-initiative-on-american-companies/> [<https://perma.cc/N4JV-9W2G>].

²²⁹ *Internet Society Statement on U.S. Clean Network Program*, INTERNET SOC’Y (Aug. 7, 2020), <https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-s-clean-network-program/> [<https://perma.cc/G7P2-EEAQ>].

²³⁰ JAMES MANYIKA AND CHARLES ROXBURGH, MCKINSEY GLOB. INST., *THE GREAT TRANSFORMER: THE IMPACT OF THE INTERNET ON ECONOMIC GROWTH AND PROSPERITY 1* (Oct. 2011), https://www.mckinsey.com/~media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.pdf [<https://perma.cc/342V-QBZY>].

neutrality,”²³¹ pointed out that Western countries have allowed “Chinese censorship and blocking of content from abroad while allowing Chinese companies to explore and exploit whatever markets it likes. Few foreign companies are allowed to reach Chinese citizens with ideas or services, but the world is fully open to China’s online companies.”²³² This begs the question, “[i]f China refuses to follow the rules of the open internet, why continue to give it access to internet markets around the world?”²³³

China has already responded to both the Trump Administration’s ban on TikTok and the Administration’s “Clean Network” initiative.²³⁴ First, China implemented its own rules governing Chinese tech companies’ sales to foreign entities by requiring that companies receive a license from local commerce authorities before engaging in such a transaction.²³⁵ Additionally, China introduced its own “Global Initiative on Data Security.”²³⁶ The Chinese Foreign Ministry announced that the initiative would aim to encourage all countries to deal with data in “‘a comprehensive, objective and evidence-based manner’ and maintain an open, secure and stable supply chain for information and communications technology and services”²³⁷ The initiative would also encourage countries to “respect other countries’ sovereignty in how they handle data”—a not so subtle swing at current U.S. policy.²³⁸ China has also created an “unreliable entity

²³¹ Timothy Wu, COLUM. L. SCH., <https://www.law.columbia.edu/faculty/timothy-wu> [<https://perma.cc/L864-HJ6H>] (last visited Sept. 18, 2020).

²³² Wu, *supra* note 17.

²³³ *Id.*

²³⁴ Eva Xiao & Liza Lin, *TikTok Talks Could Face Hurdle as China Tightens Tech Export Rules*, WALL ST. J. (Aug. 30, 2020, 10:41 AM), <https://www.wsj.com/articles/china-tightens-ai-export-restrictions-11598703527> [<https://perma.cc/KLP4-KKCL>].

²³⁵ *Id.*

²³⁶ Chun Han Wong, *China Launches Initiative to Set Global Data-Security Rules*, WALL ST. J. (Sept. 8, 2020, 12:06 AM), <https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974?mod=searchresults&page=1&pos=13> [<https://perma.cc/T6KF-2P8J>].

²³⁷ *Id.*

²³⁸ *Id.*

list,” similar to the U.S. Commerce Department’s Entity List.²³⁹ The list will include companies that threaten the “national sovereignty, security or development interests of China,” along with companies who suspend “normal transactions” or take “discriminatory measures” against Chinese companies.²⁴⁰

D. The Biden Administration’s Approach

Despite the election of a new President and the dissipation of the immediate threat of a ban (pending the Biden’s Administration’s review), it is clear that many of the circumstances that led to the proposed TikTok ban have not changed. In fact, the situation could foreshadow the beginning of the end of Chinese tech in the United States.²⁴¹ There is clear bipartisan support for policies that target China.²⁴² The policy positions of the Republican and Democratic 2020 Presidential candidates were a good example of this.²⁴³ Leading up to the election, commentators speculated that Biden would continue Trump’s trend of attempting “to mitigate foreign ownership of Chinese companies in the United States.”²⁴⁴ The

²³⁹ Evelyn Cheng, *China Releases Details on its Own Blacklist, Raising Uncertainty for Foreign Businesses*, CNBC (Sept. 21, 2020, 2:56 AM), <https://www.cnbc.com/2020/09/21/china-releases-details-on-unreliable-entity-list-raising-uncertainty-for-foreign-businesses.html> [<https://perma.cc/MR9A-8WH3>].

²⁴⁰ *Id.*; Provisions on the Unreliable Entity List (promulgated by the Ministry of Commerce, effective Sept. 19, 2020) No. 4 <http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml> [<https://perma.cc/8RKS-RGYR>] (China).

²⁴¹ See Jay Peters, *Biden’s Staff Must Delete TikTok from Their Personal and Work Phones*, THE VERGE (July 27, 2020, 9:05 PM), <https://www.theverge.com/2020/7/27/21341062/biden-staff-delete-tiktok-personal-work-phones> [<https://perma.cc/5WF3-6UME>].

²⁴² Naomi Xu Elegant, *How Anti-Beijing Legislation Became One of the Few Things Democrats and Republicans Can Agree On*, FORTUNE (Dec. 26, 2020, 6:30 AM), <https://fortune.com/2020/12/26/delisting-chinese-companies-law-china-congress-trump/> [<https://perma.cc/Z7M3-L8HL>].

²⁴³ Ben Werschkul, *Why 2020 Election May Show There’s Not Much Difference Between Trump, Biden on China Policy*, YAHOO! FIN. (Aug. 24, 2020), <https://finance.yahoo.com/news/why-2020-election-may-show-theres-not-much-difference-between-trump-biden-on-china-policy-133829561.html> [<https://perma.cc/SU9V-5B8P>].

²⁴⁴ Ben Werschkul, *Why Biden May Not Differ from Trump When it Comes to TikTok*, YAHOO! FIN. (Aug. 31, 2020), <https://finance.yahoo.com/news/why->

commentators took this position because both Biden and Trump believe that “China’s been cheating, both think China has been stealing U.S. intellectual property, both want to continue a very kind of strong arm approach towards China.”²⁴⁵ When examining both former candidates’ approaches to foreign policy, there was no real distinction in the substance of the policy each candidate wished to pursue regarding China.²⁴⁶

President Biden’s Administration has already taken steps that seemingly confirm the commentators’ speculations. For example, the first meeting between Chinese and U.S. officials under the Biden Administration began with an exchange of insults between the respective parties.²⁴⁷ Additionally, Biden’s Commerce Department allowed a Trump Administration rule restricting importation of Chinese tech to go into effect on March 22, 2021.²⁴⁸ Foreign tech companies need to adjust quickly to what likely will be the new normal.

Foreign tech companies should use TikTok as a lesson and begin whatever mitigation they can immediately. At the very least, companies should be prepared to work closely with CFIUS regarding any foreign transactions that occur that could implicate U.S. national security. Companies will likely have to engage in extreme transparency efforts (even though it has not exactly worked out smoothly for TikTok), especially concerning where data is

biden-may-not-differ-from-trump-when-it-comes-to-tik-tok-161013404.html
[<https://perma.cc/SK3V-A3Q8>].

²⁴⁵ Werschkul, *supra* note 243.

²⁴⁶ *Id.*

²⁴⁷ Evelyn Cheng, *First U.S.-China Meeting Under Biden Gets Off to a Rocky Start*, CNBC (Mar. 19, 2021, 3:07 AM), <https://www.cnbc.com/2021/03/19/-first-us-china-meeting-under-biden-gets-off-to-a-rocky-start.html> [<https://perma.cc/BME8-7ZS3>].

²⁴⁸ Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,909 (Jan. 19, 2021) (to be codified at 15 C.F.R. pt. 7); David Shepardson et al., *Biden on Track to Apply Trump-era Rule Targeting Chinese Tech Supply Chain Concerns*, REUTERS (Feb. 26, 2021, 1:37 PM), <https://www.reuters.com/article/us-usa-china-tech/biden-on-track-to-apply-trump-era-rule-targeting-chinese-tech-supply-chain-concerns-idUSKBN2AQ2PL> [<https://perma.cc/9B8K-TFWY>].

stored and who can access that data.²⁴⁹ Despite the intense competition, tech companies will likely need to work together to develop workable solutions and best practices concerning data security issues.²⁵⁰ If these companies fail to develop industry-wide standards, the consequences will be significant, and net nationalism will control. Implementing a “Clean Network” will force companies to operate their businesses in dramatically different fashions, if at all, depending on the country in which the company is located.

E. Possible Solutions

If a foreign tech company engages in any activity or association that may be perceived as a threat to U.S. national security, then that company should take necessary steps to mitigate that threat. Mitigating such threats will be necessary to continue doing business in the United States, as well as hopefully contribute to the sustainability of the open, global internet. To begin, upon reviewing the legal framework in place to ban apps, foreign tech companies must take a more proactive approach in dealing with CFIUS to counter CFIUS’ own, more active, approach. For example, if an acquisition raises the possibility of implicating national security concerns, any foreign company that acquires an interest in or

²⁴⁹ For example:

TikTok implemented several practices to mitigate the risks, including: storing U.S. user data in the U.S. and backing it up on Singaporean servers, blocking access to its data from its mother company ByteDance, hiring an American CEO and operations team, beefing up its lobbying team, withdrawing from Hong Kong based on the concerns over China’s new national security law, launching a “transparency center” for moderation and data practices in Los Angeles, banning political and advocacy advertising from its platform, and setting up a global headquarters outside of China.

Keman Huang & Stuart Madnick, *The TikTok Ban Should Worry Every Company*, HARV. BUS. REV. (Aug. 28, 2020), <https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company> [<https://perma.cc/EH3L-PKPD>].

²⁵⁰ Most recently, TikTok has called on Instagram and Facebook to help fight the ban. See Julia Alexander, *TikTok CEO Asks Instagram, Facebook to Help Fight TikTok Ban*, THE VERGE (Sept. 18, 2018, 11:32 AM), <https://www.theverge.com/2020/9/18/21445321/tiktok-trump-ban-instagram-facebook-adam-mosseri-app-store-google-play> [<https://perma.cc/6WG5-N877>].

purchases a U.S. company should notify CFIUS, formally or informally.

Some mitigation strategies aimed at lowering the threat to national security include ensuring that only U.S. citizens have access to critical functions and decisions of the company, imposing independent audit requirements, and being more open to government oversight.²⁵¹ Additionally, foreign companies should store user data on clouds and servers that are trusted “clean” vendors. If these companies want to be exceptionally safe in the eyes of the U.S. government, companies should not store any user data in China. This practice would help assure the U.S. government that American data is not accessible to foreign governments for espionage or other purposes that may raise national security concerns.

Additionally, companies should publish information on how their company handles user data. This publication should include (1) where data is stored, (2) if the company may sell data to third parties, and (3) when companies would be required to hand over the data to government or law enforcement authorities. Also, tech companies should grant government and regulatory agencies access to their code in order to test for security loopholes or concerns. TikTok has already offered this oversight option to the Australian government in an attempt to ease distrust, and TikTok had planned to allow Oracle to inspect its code before negotiations were put on pause.²⁵²

Next, companies should be exceedingly open and transparent about their content moderation as a good faith effort to facilitate trust. The Santa Clara Principles on Transparency and Accountability in Content Moderation (“Santa Clara Principles”) provide an adequate beginning framework for companies wishing to

²⁵¹ LATHAM & WATKINS LLP, *supra* note 77, at 8.

²⁵² Kirsty Needham, *TikTok Tells Australia Government it Will Make Source Code Available for Inspection*, REUTERS (Sept. 25, 2020, 3:56 AM), <https://www.reuters.com/article/us-usa-tiktok-australia/tiktok-tells-australia-government-it-will-make-source-code-available-for-inspection-idUSKCN26G0YM> [<https://perma.cc/8ZAU-RLV6>]; Schuetz, *supra* note 44.

improve their transparency in this regard.²⁵³ The Santa Clara Principles advise that:

Companies should publish the numbers of posts removed and accounts permanently or temporarily suspended due to violations of their content guidelines[. . .] . . . provide notice to each user whose content is taken down or account is suspended about the reason for the removal or suspension . . . [and] provide a meaningful opportunity for timely appeal of any content removal or account suspension.²⁵⁴

Company transparency will likely foster trust between companies, consumers, and regulating authorities. Another benefit of company transparency and accountability is that insight would be provided on how these companies handle misinformation, which is another growing threat to national security.²⁵⁵ This transparency could alleviate government national security concerns regarding propaganda because it would clarify whether or not foreign governments are inappropriately moderating information to align with their interests.²⁵⁶

Lastly, tech companies should cooperatively work together to engage foreign governments and advocate for open policies. Although the competition is fierce among tech companies, the

²⁵³ *The Santa Clara Principles on Transparency and Accountability in Content Moderation*, SANTA CLARA PRINCIPLES, <https://santaclaraprinciples.org/cfp/> [<https://perma.cc/LAZ2-WL3N>] (last visited Oct. 21, 2020).

²⁵⁴ *Id.*

²⁵⁵ *Id.*; Rachel E. Greenspan, *The QAnon Conspiracy Theory and a Stew of Misinformation Fueled the Insurrection at the Capitol*, INSIDER (Jan. 7, 2021, 3:58 PM), <https://www.insider.com/capitol-riots-qanon-protest-conspiracy-theory-washington-dc-protests-2021-1> [<https://perma.cc/26XK-W5Q9>]. The storming of the U.S. Capitol by far-right conspiracy theorists in an attempt to block then President-Elect Joe Biden from ascending to the presidency is an example of how the spread of misinformation can threaten national security. *Id.*

²⁵⁶ Sherman, *supra* note 60. Sherman states:

Again, the national security risks here are not as direct as with data collection. Yet there are genuine concerns about the Chinese government exporting its censorship through platforms like TikTok. The worry is that Beijing compels high-demand Chinese-incorporated internet platforms to remove content worldwide. Beijing's internet censorship practices, otherwise confined within Chinese borders, could hypothetically spread through this tactic.

Id.

existence of a free and open internet where citizens from all countries can exchange ideas is more important. Tech companies should encourage countries to be democratic in how they handle their citizen's data and access to the internet and should not seek out authoritarian policies that act purely as an Orwellian "big brother." Tech companies should pressure countries that do so, like China or Iran, and encourage the United States and other Western countries to not falter in their commitment to protect a democratic, open internet, while understanding that there still must be a way to address legitimate national security concerns.

V. CONCLUSION

The attempted TikTok ban has provided a valuable example of the power available to the Executive Branch to ban a foreign company's operations within the United States. It has implicated the unsettled question of whether the First Amendment applies to a social media app that is possibly tainted with foreign control or influence in U.S. government's eyes. It is clear that the protection of American data is an essential objective of the U.S. government, and foreign companies will continuously have to adjust to persuade the United States government that they are not a threat. As evidenced in the possible implementation of the "Clean Network," the move towards net nationalism offers insight into a world that may soon have to choose between the Chinese or the American sphere of internet influence.

Although the foreign business and policy implications are tremendous, a TikTok ban is more than just a legal fight. It is the conflation of economic, trade competition, and national security concerns that happened to come together in one of the most dramatic ways possible. The executive branch can and will act against foreign tech companies perceived to be a threat to national security—a rapidly expanding category. The implications could mean a world where what is available to users online depends on what that user's government has deemed appropriate. The competing spheres of the Chinese and American internet could cripple global free markets and trade. It is on tech to work together to address the "splintering" of the internet and adopt workable solutions before it is too late. TikTok might have almost been the first foreign company to fall to

net nationalism; but, if these trends continue, it certainly will not be the last.