Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 16
Issue 1 *SYMPOSIUM A Life Navigating the Securities Markets: A Celebration of Professor Roberta Karmel's Work, Teaching, and Mentorship*

Article 11

12-1-2021

When Your Apps Threaten National Security – A Review of the TikTok and WeChat Bans and Government Actions Under IEEPA and FIRRMA

Ru Hochen

WHEN YOUR APPS THREATEN NATIONAL SECURITY—A REVIEW OF THE TIKTOK AND WECHAT BANS AND GOVERNMENT ACTIONS UNDER IEEPA AND FIRRMA

ABSTRACT

Personal data can evolve into a national security issue. In August 2020, fears of foreign adversaries' access to Americans' personal data prompted President Trump to issue two executive orders that attempted to ban Chinese-owned social media applications TikTok and WeChat in the United States. In the last few years, the U.S. executive branch has acted against foreign entities that implicate national security interests via two primary tools: the presidential power under the International Economic Emergency Powers Act (IEEPA) and a foreign investment screening regime under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). However, the statutes were enacted before Congress could have envisioned the impact of personal information on national security. IEEPA's statutory limitations especially make it an ill-fitting tool to regulate software data ownership and acquisitions. This Note will review recent uses of IEEPA and FIRRMA, analyze the legal problems and economic implications of the TikTok-WeChat ban, and propose that FIRRMA serves as a better solution to address data privacy risks posed by software and that further statutory reforms are necessary to better protect the nation's and people's interests.

INTRODUCTION

It might be difficult to associate the idea of a national security crisis with a social media application (app) on your phone. However, the U.S. federal government first officially noted the potential threat to national security posed by a communications service in May 2019, when President Trump declared a national emergency involving the vulnerabilities in information and communications technology exploited by foreign adversaries.[1] Subsequently, on August 6, 2020, President Trump issued two Executive Orders (EO(s)), addressing the threats posed by the two mobile apps, TikTok and WeChat,[2] by barring future transactions with their Chinese parent

1. Exec. Order No. 13,873, 3 C.F.R. § 317 (2020) (stating that "foreign adversaries are . . . exploiting vulnerabilities in information and communications technology and services" and that their unrestricted acquisition and use of such technology constitutes an unusual and extraordinary threat to national security).

2. *See generally* Exec. Order No. 13942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) [hereinafter TikTok EO] (addressing the threat posed by TikTok); Exec. Order No. 13943, 85 Fed. Reg. 48,641 (Aug. 6, 2020) [hereinafter WeChat EO] (addressing the threat posed by WeChat). For a brief history of the TikTok and WeChat bans, the Trump administration issued another EO on August 14, 2020, mandating TikTok to either follow the TikTok EO or sell its U.S. business to a U.S. company. After the EOs were issued, TikTok, TikTok's users, and WeChat's users each brought a lawsuit, claiming that the TikTok-WeChat ban violated the First Amendment and the International

companies ByteDance and Tencent.[3] TikTok is a popular video-sharing social networking platform that has reached over one billion monthly users worldwide,[4] while WeChat is an extremely prevalent multi-purpose messaging app in Chinese communities, with over one billion monthly users around the world.[5]

In both EOs, President Trump invoked the International Emergency Economic Powers Act (IEEPA) as his legal authority.[6] Under IEEPA, the president of the United States is entitled to deal with any "unusual and extraordinary threat" to the U.S. national security or economy after declaring a national emergency with respect to such threat.[7] Reiterating the emergency announced in May 2019, President Trump alleged that the two apps capture vast swaths of user information and grant the Chinese Communist Party (CCP) access to Americans' personal information,[8] which may be used for blackmail, espionage, and disinformation campaigns that benefit the CCP.[9] The Trump administration believed that the use of the two apps continued to threaten the U.S. security and economy, thus warranting a ban on the

Emergency Economic Powers Act (IEEPA), among other things. The courts ultimately granted an injunction in late 2020, enjoining the Trump administration from implementing the prohibitions. On June 9, 2021, President Biden officially revoked both TikTok and WeChat EOs but instructed the federal government to further evaluate the threats. *See infra* notes 18, 131, 135, and 188–192 and accompanying text.

3. TikTok's EO bars any transaction with the app's parent company ByteDance or its subsidiaries, while WeChat's EO bars any transaction related to WeChat with its parent company Tencent or its subsidiaries as identified by the Secretary of Commerce. TikTok EO, *supra* note 2; WeChat EO, *supra* note 2.

4. Having gained great success in recent years, TikTok has reportedly been downloaded over 175 million times in the United States and has reached one billion monthly users around the world as of September 2021. *See* TikTok EO, *supra* note 2; *Thanks a Billion!* TIKTOK (Sept. 27, 2021), https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok.

5. WeChat is owned by Chinese company Tencent and has over a billion monthly users worldwide as of 2019. For Chinese users, it is a "super app" that provides for calling, messaging, social media, mobile payment, and news feed services. *See* Arjun Kharpal, *Everything You Need to Know About WeChat*, CNBC (Feb. 4, 2019), https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html; *see also* Heather Kelly & Emily Rauhala, *What a WeChat Ban Could Mean for Millions of U.S. Users*, WASH. POST (Sept. 18, 2020), https://www.washingtonpost.com/technology/2020/09/18/wechat-ban-faq/.

6. *See generally* International Emergency Economic Powers Act, Pub. L. No. 95-223, 91 Stat. 1625 (1977) (codified as amended at 50 U.S.C. §§ 1701–1706). The order also refers to other statutes, but IEEPA is the most crucial one. *See* TikTok EO, *supra* note 2; WeChat EO, *supra* note 2.

7. 50 U.S.C. § 1701(a) ("[The president is entitled] to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the president declares a national emergency with respect to such threat.").

8. *See* TikTok EO, *supra* note 2; WeChat EO, *supra* note 2.

9. TikTok EO, *supra* note 2 (claiming that TikTok's data collection "potentially allow[s] China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage" and that "TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus").

downloads of the apps and any future transactions with their foreign owners.[10]

Given the recent U.S.-China tensions[11] and a growing worldwide concern for the Chinese government's control over these two apps,[12] it is perhaps not surprising that TikTok and WeChat would attract the U.S. government's attention. Especially over the last few years, the executive branch has sanctioned Chinese entities on multiple occasions via two primary tools: (1) the presidential power under IEEPA and (2) review conducted by the Committee on Foreign Investment in the United States (CFIUS) under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[13] For instance, in 2019, President Trump used IEEPA to prohibit China's telecom giant Huawei[14] from conducting business with American companies.[15] Several Chinese investors were required to divest from

10. *See* TikTok EO, *supra* note 2; WeChat EO, *supra* note 2. *But see* Vincent Chow, *TikTok Slams US Foreign Investment Review Body in Lawsuit Filing*, LAW.COM (Aug. 27, 2020), https://www.law.com/therecorder/2020/08/27/tiktok-slams-u-s-foreign-investment-review-body-in-lawsuit-filing-403-54160/ (stating that TikTok had provided tons of information to the government about its safety measures safeguarding U.S. user data and preventing it from being accessed by unauthorized parties).

11. In July 2018, President Trump imposed tariffs on China for its alleged unfair trade practices. Since then, "the two countries have been embroiled in countless back-and-forth negotiations," tariff wars, and foreign technology restrictions, consequently leading the US-China tensions "to the brink of a full-blown trade war." For a timeline of the trade conflict, see Dorcas Wong & Alexander Chipman Koty, *The US-China Trade War: A Timeline*, CHINA BRIEFING (updated Aug. 25, 2020), https://www.china-briefing.com/news/the-us-china-trade-war-a-timeline/. The trade war paused in early 2020, but the two nations' relationship worsened following the outbreak of the 2019 Novel Coronavirus (COVID-19) in the spring of 2020 when President Trump blamed Beijing for a lack of transparency over the COVID-19 outbreak in China, while Chinese officials suggested that the virus had its origin in the United States. *See* Weizhen Tan, *US-China Relations at a Low as 'Blame-Shifting' Sets Back War Against Virus*, CNBC (Apr. 21, 2020), https://www.cnbc.com/2020/04/22/coronavirus-trump-blames-china-virus-impact-on-trade-war.html.

12. Countries such as India and Australia have banned WeChat and TikTok to some extent. *See* Maria Abi-Habib, *India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat*, N.Y. TIMES (June 30, 2020), https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html (reporting that India banned nearly 60 Chinese apps including TikTok and WeChat, citing national security concerns, after a clash between China and India's militaries in June 2020); Angus Grigg, *Australia's Defence Department Bans Chinese App WeChat*, AUSTRALIAN FIN. REP. (Mar. 11, 2018), https://www.afr.com/technology/australias-defence-department-bans-chinese-app-wechat-20180310-h0xay8.

13. CFIUS is authorized by FIRRMA to regulate certain transactions involving foreign investment in the United States. *See generally* FIRRMA, Pub. L. No. 115-232, §§ 1701-1728, 132 Stat. 1636 (codified as amended at 50 U.S.C. § 4565) (2018); CFIUS, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

14. Based in China, Huawei is the world's largest seller of smartphones and telecommunications equipment, including 5G network infrastructure. Lindsay Maizland et al., *Huawei: China's Controversial Tech Giant*, COUNSEL ON FOREIGN RELATIONS (Aug. 6, 2020), https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

15. Although the EO in May 2019 did not name any entity, in effect, it prohibits U.S. companies from sourcing telecom gear from companies that threaten national security and authorizes the Department of Commerce to ban Huawei from buying components from U.S. companies without

American businesses that possessed critical technology or sensitive personal data because of national security concerns, as advised by CFIUS.[16] In TikTok's case, months prior to the EO announced in August 2020, ByteDance was already under CFIUS's scrutiny for its acquisition of Musical.ly, a China-based platform.[17]

Despite the precedent and the growing international rivalry between the United States and China, the TikTok and WeChat bans have faced multiple challenges.[18] Specifically, TikTok brought a suit in the District Court for the District of Columbia,[19] arguing that the EO exceeded the president's power under IEEPA since the statute explicitly bars the president from restricting "personal communications" and "informational materials."[20] Further, while these bans might achieve certain political goals, scholars and corporations have raised concerns about the economic costs, as the bans directly affected

government approval. *See* Exec. Order No. 13,873, 3 C.F.R. § 317 (2020); *see also* Kendra Chamberlain, *Commerce Dept. Bans Huawei, 70 Affiliates from Sourcing U.S. Components*, FIERCE WIRELESS (May 16, 2019), https://www.fiercewireless.com/5g/commerce-dept-adds-huawei-and-70-affiliates-to-telecom-ban-list.

16. *See, e.g.*, Presidential Order Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corporation, 77 Fed. Reg. 60,281 (Sept. 28, 2012) (prohibiting Ralls, a Chinese-owned corporation, from owning and developing wind farm projects in Oregon due to national security concerns); *see also* Carl O'Donnell et al., *Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, REUTERS (Mar. 27, 2019), https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-u-s-pushes-chinese-owner-of-grindr-to-divest-the-dating-app-sources-idUSKCN1R809L (reporting that Grindr, a Chinese-owned dating app, was informed of a national security risk and ultimately divested from its U.S. business).

17. Complaint at 15, TikTok Inc. v. Trump, 490 F. Supp. 3d 73 (D.D.C. 2020) [hereinafter TikTok Complaint] (detailing that CFIUS initiated a review in June 2020 of ByteDance's 2017 acquisition of Musical.ly, a China-based video sharing platform with assets in the United States).

18. On September 18, 2020, TikTok and ByteDance filed a lawsuit in the D.C. District Court, alleging that the government's actions, among other things, exceed the president's authority under IEEPA. *See* TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 76 (D.D.C. 2020). Several prominent TikTok users also challenged the ban in Pennsylvania. *See generally* Marland v. Trump, 498 F. Supp. 3d 624 (E.D. Pa. 2020). Similarly, while Tencent itself did not file a suit, a nonprofit U.S. WeChat Users Alliance and several WeChat users sued in California, claiming the WeChat ban was unconstitutional. *See generally* U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912 (N.D. Cal. 2020). Several American corporations also voiced concern about the WeChat ban's impact on their business in China. *See* John D. McKinnon and Lingling Wei, *Corporate America Worries WeChat Ban Could Be Bad for Business,* WALL ST. J. (Aug. 13, 2020), https://www.wsj.com/articles/corporate-america-worries-wechat-ban-could-be-bad-for-business-11597311003.

19. *TikTok*, 490 F. Supp. 3d 73, 76.

20. *See generally* 50 U.S.C. § 1702(b).

the stakeholders' interests[21] and may jeopardize American business overseas by discouraging future foreign investments.[22]

Due to the legal and economic problems presented by the TikTok-WeChat ban, the executive branch should consider other alternatives to address the issue. This Note will argue that absent a more obvious "unusual and extraordinary" threat and when a government action might incur high costs, the executive branch should avoid invoking IEEPA. Instead, the government should consider taking another route, such as CFIUS, to review the national security risks posed by the foreign ownership of a platform or software that provides access to Americans' personal data. While there is certainly room for improvement in CFIUS's review process,[23] it is a better option under the current legal framework to minimize costs while serving the country's interests.

Part I of this Note will provide an overview of IEEPA and CFIUS and their recent uses in relation to Chinese-owned companies. Part II will delve into the legal problems and economic implications presented by the use of IEEPA in the TikTok-WeChat ban. Part III will propose that compared with IEEPA, CFIUS's review process is a better option to address the security concerns posed by an app; at the same time, certain reforms may be necessary to better serve each party's interests.

I. STATUTORY FRAMEWORK AND BACKGROUND OF IEEPA AND FIRRMA

A. OVERVIEW OF IEEPA

Before IEEPA, Congress passed the Trading with the Enemy Act (TWEA) during World War I, allowing the president to regulate both domestic and foreign transactions in times of peace and war.[24] In 1977, in

21. For instance, Fastly, a cloud services provider, suffered a great financial loss after ByteDance decided to pull most of its TikTok traffic from Fastly to change its operations in response to the TikTok ban. *See* Isabelle Lee, *ByteDance Pulls Most of Its TikTok Traffic from Fastly Network*, BLOOMBERG (Oct. 29, 2020), https://www.bloomberg.com/news/articles/2020-10-28/fastly-quarterly-sales-forecast-meets-wall-street-expectations; *see also* Tiernan Ray, *Fastly Plunges 37% as Customer ByteDance, TikTok Owner, Hit by Geopolitics*, ZDNET (Oct. 14, 2020), https://www.zdnet.com/article/fastly-plunges-37-as-tiktok-parent-bytedance-hit-by-u-s-ban/ (describing that Fastly's stock plunged 37% due to the impacts of the uncertain geopolitical environment).

22. McKinnon & Wei, *supra* note 18; Jeremy Straub, *The US Has Lots to Lose and Little to Gain by Banning TikTok and WeChat*, CONVERSATION (Aug. 28, 2020), https://theconversation.com/the-us-has-lots-to-lose-and-little-to-gain-by-banning-tiktok-and-wechat-144478.

23. *See generally* E. Maddy Berg, *A Tale of Two Statutes: Using IEEPA's Accountability Safeguards to Inspire CFIUS Reform*, 118 COLUM. L. REV. 1763 (2018) (highlighting the accountability concerns in CFIUS's framework).

24. In 1917, Congress passed TWEA, authorizing the president to regulate international transactions with enemies during times of war as declared by Congress. Over the years, Congress amended TWEA, allowing the president to declare a national emergency in times of peace and giving the president sweeping powers to regulate both domestic and foreign transactions. CONG.

light of the overly broad presidential authority under TWEA, Congress enacted IEEPA as a new vehicle for adopting economic control during times of declared national emergency.[25] Under IEEPA, the president is empowered, among other things, to regulate or prohibit any transactions involving a foreign-owned property that is subject to U.S. jurisdiction.[26]

To protect the American people's right to engage in personal communication with a foreign person, Congress added a few limitations in the statute.[27] Specifically, IEEPA cannot be used to regulate "any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value."[28] Nor can the president take advantage of IEEPA to regulate the importation or exportation of "any information or informational materials," such as publications, films, and news wire feeds.[29] More importantly, to exercise the emergency powers, the president must first declare a national emergency based on an "unusual and extraordinary threat" to the country's security or economy.[30] If the president determines that the emergency continues to exist, he must report to Congress every six months on the use of such authority.[31]

Although IEEPA was intended to be used only in truly urgent and extraordinary circumstances,[32] the use of IEEPA has expanded in scope and frequency since the statute's enactment.[33] The terms "national emergency" and "unusual and extraordinary threat" are not defined in the statute, which has provided the executive significant leeway.[34] Over the past few decades,

---

RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE, at 4–5 (2020) [hereinafter CRS Report].

25. After discovering that the United States had been in a state of emergency for over 40 years under TWEA, Congress amended TWEA by eliminating certain presidential authority in times of declared national emergency and enacted IEEPA. *See* CRS Report, *supra* note 24, at 7–8.

26. *See* 50 U.S.C. § 1702(a)(1)(B) ("[The president may] investigate . . . or prohibit any acquisition . . . or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United State.").

27. *See generally* 50 U.S.C. § 1702(b); *see also* CRS Report, *supra* note 24, at 12.

28. 50 U.S.C. § 1702(b)(1).

29. 50 U.S.C. § 1702(b)(3) (providing an exception for "the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds").

30. 50 U.S.C. § 1701(a).

31. 50 U.S.C. § 1706(d).

32. *See* CRS Report, *supra* note 24, at 44; *see also* Andrew Boyle, *Checking the President's Sanctions Powers*, BRENNAN CENTER FOR JUSTICE 3 (June 10, 2021) [hereinafter Boyle, *Checking the President's Sanctions Powers*].

33. *See* CRS Report, *supra* note 24, at 17–18 (describing how IEEPA has been invoked 59 times in declared emergencies as of July 1, 2020, and that in addition to foreign governments, the U.S. administrations have increasingly used IEEPA to target individuals and groups engaging in malicious cyber-enabled activities).

34. *See* Andrew Boyle, *An Emergency or Business as Usual? Huawei and Trump's Emergency Powers*, JUST SECURITY (May 24, 2019), https://www.justsecurity.org/64252/an-emergency-or-

national emergencies have ranged from a hostage crisis in Iran[35] to foreign interference in a U.S. election,[36] unlawful immigration across the southern border,[37] and the exploitation of certain U.S. information and technology.[38] IEEPA has somehow become a routinely used foreign policy tool, which may "cheapen the currency of national emergencies."[39]

In TikTok and WeChat's case, as mentioned earlier, the bans were based on the national emergency declared in May 2019 involving foreign threats to U.S. information and communication technology.[40] That emergency order came amid the battle between the United States and Huawei, when Huawei planned to deploy 5G networks worldwide with its equipment.[41] The American government had been concerned about the security of Huawei's equipment since 2012,[42] when a Congressional report found that Huawei "cannot be trusted to be free of foreign state influence" and that "provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests."[43] Further, in January 2019, U.S. prosecutors charged Huawei for conspiring to steal T-Mobile's trade secrets, and Huawei and its Chief Financial Officer were charged with bank and wire fraud in violation of American sanctions on Iran.[44] The U.S. administration was likely

business-as-usual-huawei-and-trumps-emergency-powers/ [hereinafter Boyle, *Emergency or Business*] (noting that presidents have been interpreting the undefined terms and IEEPA's emergency power in their favor).

35. Exec. Order No. 12,170, 3 C.F.R. § 457 (1980) (declaring a national emergency with regards to the hostage situation in Iran).

36. Exec. Order No. 13,848, 3 C.F.R. § 869 (2019) (declaring a national emergency based on foreign persons' ability to interfere in U.S. elections, which is magnified by the proliferation of digital devices and online communications).

37. Proclamation No. 9844, 84 Fed. Reg. 4949 (Feb. 15, 2019) (announcing a national emergency posed by a "long-standing" border security and humanitarian crisis resulting from the southern border's role as "a major entry point for criminals, gang members, and illicit narcotics").

38. Exec. Order No. 13,873, 3 C.F.R. § 317 (2020).

39. Boyle, *Emergency or Business*, *supra* note 34.

40. *See generally* Exec. Order No. 13,873, 3 C.F.R. § 317 (2020).

41. *See Huawei Has 22 Commercial 5G Contracts; U.S. Government Warns Allies About the Company*, IEEE COMM. SOC'Y (Nov. 23, 2018), https://techblog.comsoc.org/2018/11/23/huawei-has-22-commercial-5g-contracts-u-s-government-warns-allies-about-the-company/.

42. *See* Kendra Chamberlain, *Trump to Ban U.S. Carriers from Using Network Gear Posing Security Risk: Reuters*, FIERCE WIRELESS (May 15, 2019), https://www.fiercewireless.com/tech/trump-to-direct-us-carriers-to-ban-network-gear-pose-security-risk-reuters.

43. STAFF OF H.R. PERMANENT SELECT COMM. ON INTEL., 112TH CONG., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE, at iv–vi, (Comm. Print 2012) (written by Mike Rogers, Chairman, & C.A. Dutch Ruppersberger, Ranking Member, H.R. Permanent Select Comm. on Intel.), available at https://intelligence.house.gov/news/documentsingle.aspx (summarizing that Huawei and ZTE, the top two Chinese telecoms companies, failed to provide sufficient evidence to ameliorate concerns about the safety of the equipment and potential ties to the Chinese government or military).

44. *See Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud*, U.S. DEP'T JUSTICE (Jan. 28, 2019), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial (detailing that Huawei was charged with bank fraud, violating the IEEPA, and

prompted by these events to block Huawei from entering the country.[45] In May 2019, President Trump issued an EO authorizing the Secretary of Commerce to block transactions of communications technology or services with foreign entities, like Huawei, that pose an "unacceptable risk to the national security of the United States."[46]

B. OVERVIEW OF CFIUS AND FIRRMA

In addition to IEEPA, CFIUS is another instrument to regulate foreign investment. In 1975, in response to increasing foreign investment especially from Arab states,[47] President Ford created CFIUS to monitor the impact of foreign investment in the United States.[48] CFIUS is an interagency body[49] authorized to conduct a national security review of investments that could result in foreign control of a U.S. business.[50]

The review process generally works as follows. CFIUS can unilaterally initiate a review of a pending or even completed transaction[51] covered by FIRRMA.[52] Parties may also voluntarily submit a request for CFIUS's approval of a deal before it materializes.[53] Upon receiving a review request, CFIUS will inform the parties of a forty-five-day review schedule, the outcome of the review, and a follow-up investigation if necessary.[54] Once CFIUS has determined that there is no unresolved risk, the transaction

conspiracy to commit money laundering, etc., while the CFO Meng was charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud).

45. David Shepardson, *Trump Expected to Sign Order Paving Way for U.S. Telecoms Ban on Huawei*, REUTERS (May 14, 2019) https://www.reuters.com/article/us-usa-china-huawei-tech-exclusive/exclusive-trump-expected-to-sign-order-paving-way-for-u-s-telecoms-ban-on-huawei-idUSKCN1SK2P1 (mentioning that Trump was hesitant in December 2018, but the order was reportedly imminent in February 2019).

46. David R. Allman, *Scalpel or Sledgehammer? Blocking Predatory Foreign Investment with CFIUS or IEEPA*, 10 AM. U. NAT'L SEC. L. BRIEF 267, 331–32 (2020).

47. Berg, *supra* note 23, at 1768.

48. *See* Exec. Order No. 11,858, 3 C.F.R. § 990 (1975).

49. The Secretary of the Treasury serves as the chairperson of CFIUS, and the members include heads from the following departments and offices: Departments of Justice, Homeland Security, Commerce, Defense, State, and Energy, as well as the Office of the U.S. Trade Representative and Office of Science and Technology Policy. *CFIUS Overview*, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview (last visited Sept. 22, 2021).

50. *See* 50 U.S.C. § 4565(a)(4)(B)(iv)(I); *see also CFIUS Laws and Guidance*, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance (last visited Oct. 3, 2021) (enumerating the categories of transactions subject to CFIUS's review, such as any merger or acquisition that could result in foreign control of a U.S. business).

51. There is no statute of limitations preventing CFIUS from retroactively reviewing past transactions. *See generally* 50 U.S.C. § 4565; Jonathan Wakely & Andrew Indorf, *Managing National Security Risk in an Open Economy: Reforming the Committee on Foreign Investment in the United States*, 9 HARV. NAT'L SEC. J. 1, 8 (2018).

52. 50 U.S.C. § 4565(b)(1)(D).

53. *See CFIUS Overview*, *supra* note 49.

54. *Id.*

receives a legal "safe harbor," and CFIUS is generally estopped from reviewing the transaction again except in very limited circumstances.[55]

If a risk exists, the president, not CFIUS, has the authority to prohibit the transaction.[56] On the other hand, CFIUS may impose certain conditions with regard to the transaction to mitigate the risk,[57] such as excluding sensitive assets from the scope of the transaction, limiting parties' access to certain data, and enhancing data security measures.[58] Alternatively, CFIUS can refer a particular case for the president's review.[59] The president then must announce a decision within fifteen days following the completion of CFIUS's investigation or referral of the case.[60] The president has discretion on whether to follow CFIUS's recommendation to suspend or prohibit the transaction.[61]

CFIUS has served as a gatekeeper to "manage the national security risks inherent to the major role the United States plays in the world economy."[62] Its power has been further strengthened due to the newly perceived threats posed by America's weakened economic position.[63] In August 2018, against the backdrop of the U.S.-China trade war,[64] Congress passed FIRRMA,[65] expanding CFIUS's jurisdiction over certain types of transactions, including foreign investments involving critical infrastructure, critical technology, or businesses that maintain or collect sensitive personal data of U.S. citizens that could be exploited in a manner that threatens national security.[66] FIRRMA further provides factors for CFIUS and the president to consider in determining national security risks, such as whether the transaction involves "a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security."[67]

55. *See, e.g.*, 50 U.S.C. § 4565(b)(1)(D)(ii) (prohibiting CFIUS or the president from reviewing a transaction again unless the party submitted false or misleading material information or omitted material information).

56. 50 U.S.C. § 4565(d); Wakely & Indorf, *supra* note 51, at 32.

57. *CFIUS Overview*, *supra* note 49.

58. Wakely & Indorf, *supra* note 51, at 32–33.

59. *CFIUS Overview*, *supra* note 49.

60. 50 U.S.C. §4565(d)(2).

61. 50 U.S.C. §4565(d).

62. Allman, *supra* note 46, at 271.

63. Berg, *supra* note 23, at 1769–70 (describing that the threats—the United States' declining economic position and a worsening trade relationship with Japan—urged Congress to pass the Exon-Florio Amendment of 1988, which authorized the president to investigate and block foreign "mergers, acquisitions, or takeovers" absent the national-emergency declaration required under CFIUS's IEEPA-era regime).

64. *Id.* at 1773–74.

65. *See generally* 50 U.S.C. § 4565; *see also CFIUS Laws and Guidance*, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance (last visited Oct. 3, 2021) (explaining that the president's authority to suspend or prohibit certain transactions was initially provided by Section 721 of the Defense Production Act of 1950, which was substantially revised by FIRRMA).

66. 50 U.S.C. § 4565(a)(4)(B)(iii).

67. FIRRMA § 1702(c)(1).

While no specific countries are referenced, as scholars have observed, the language allows CFIUS to potentially target specific foreign investors by country of origin in its foreign investment regime.[68]

These amendments have enabled CFIUS to focus its attention on investments that would result in Chinese entities' access to Americans' personal data.[69] For instance, Grindr, an LGBTQ dating app acquired and owned by a Chinese company between 2016 and 2018,[70] was divested from its parent company in March 2020 under pressure from CFIUS.[71] Although CFIUS did not publicly comment on this action, the committee reportedly worried that the Chinese government could use the sensitive personal data such as geolocation, sexual preferences, and HIV status acquired through the app[72] to blackmail American citizens and government officials, thereby endangering national security.[73] Similarly, in April 2019, PatientsLikeMe, an online health platform that connects patients with similar medical conditions, was forced into a fire sale due to national security concerns posed by its major Chinese investor's potential access to Americans' sensitive health data.[74] Further, in March 2020, on CFIUS's recommendation, President Trump ordered China-based Beijing Shiji Information Technology to sell off

68. JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS), at 2, 13 (2020); Adam Chan, *CFIUS, Team Telecom and China,* LAWFARE (Sept. 28, 2021), https://www.lawfareblog.com/cfius-team-telecom-and-china.

69. *See* Chan, *supra* note 68.

70. Chinese company Kunlun acquired approximately 60% of Grindr in 2016 and bought out the remainder of the company in 2018. Echo Wang, *China's Kunlun Tech agrees to U.S. demand to sell Grindr gay dating app*, REUTERS (May 13, 2019), https://www.reuters.com/article/us-grindr-m-a-beijingkunlun-idUSKCN1SJ28N; *CFIUS Developments: Notable Cases and Key Trends*, GIBSON DUNN (Apr. 24, 2019), https://www.gibsondunn.com/cfius-developments-notable-cases-and-key-trends/.

71. CFIUS set a deadline for Kunlun to sell Grindr by June 2020. *See* Wang, *supra* note 70. *See* Jay Peters, *Grindr Has Been Sold by Its Chinese Owner After the US Expressed Security Concerns*, VERGE (Mar. 6, 2020), https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq.

72. Data including a person's photo, sexual orientation, HIV status, and geolocation are central to the use of the app. Robert Kim, *ANALYSIS: CFIUS Scrutiny Forces Chinese Sale of Grindr*, BLOOMBERG L. ANALYSIS (Apr. 16, 2019), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-cfius-scrutiny-forces-chinese-sale-of-grindr; *see also* GIBSON DUNN *supra* note 70 ("Although CFIUS has not commented publicly, observers have speculated that the action was prompted by concerns over Kunlun's access to sensitive personal data from Grindr users—such as location, sexual preferences, HIV status and messages exchanged via the Grindr app.").

73. Kim, *supra* note 72 (noting that Grindr data might have been used against U.S. officials as early as 2015 when a user outed a Republican member by leaking his Grindr photos and that foreign intelligence mining Grindr data could endanger national security).

74. Christina Farr & Ari Levy, *The Trump Administration is Forcing This Health Startup that Took Chinese Money into a Fire Sale*, CNBC (Apr. 4, 2019), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html (describing that PATIENTSLIKEME potentially presented data security risks as the company collected users health data and that in 2017, it sold a majority stake to a Chinese company called iCarbonX for its artificial intelligence technology to improve its customers and data sets).

StayNTouch, a U.S. software company it acquired in 2018.[75] Although no specific reason was given in the order, since StayNTouch serves as a property management platform for hotel chains and casinos, commentators have speculated that the government might have been concerned about Shiji's access to the guests' personal and financial records through StayNTouch, as the order specifically required Shiji to divest all interests in the latter's data, including customer data.[76]

In these cases, following CFIUS's suggestions, Grindr, PatientsLikeMe, and Shiji respectively sold their businesses to American companies,[77] thereby allowing the platforms to continue operation in the United States. PatientsLikeMe has become the world's largest real-world data platform for patients to share their stories and health information for peer support and learning.[78] Grindr has evolved into a central networking app for the LGBTQ community.[79] StayNTouch has continued to operate as a hotel property management system after being sold to a major U.S. hotel operator in August 2020.[80] Apparently, the problem was not with the platforms themselves; rather, it was their security risks, which were mitigated after a change of ownership.

II. PROBLEMS: THE STATUTORY LIMITATIONS OF IEEPA AND ECONOMIC IMPLICATIONS OF THE BAN

After examining the legal framework of IEEPA and CFIUS's review, the following section discusses two major problems in the TikTok-WeChat ban — (1) whether the ban was a lawful exercise of presidential powers under IEEPA; and (2) in light of the ban's economic impact, whether there are other less harmful alternatives to achieve the government's goal.

75. Presidential Order Regarding the Acquisition of StayNTouch, Inc. by Beijing Shiji Information Technology Co., Ltd., 85 Fed. Reg. 13,719 (Mar. 6, 2020).

76. Chan, *supra* note 68.

77. Echo Wang et al., *Winning bidder for Grindr has ties to Chinese owner*, REUTERS (June 2, 2020), https://www.reuters.com/article/us-grindr-m-a-sanvicente-exclusive/exclusive-winning-bidder-for-grindr-has-ties-to-chinese-owner-idUSKBN2391AI ("CFIUS had cleared the sale of Grindr to San Vicente Acquisition"); Matthew Herper, *PatientsLikeMe, Forced by U.S. to Ditch Chinese Investor, Sold to UnitedHealth Group*, STAT (June 24, 2019), https://www.statnews.com/2019/06/24/patientslikeme-forced-by-u-s-to-ditch-chinese-investor-sold-to-unitedhealth-group/; Katy Stech Ferek, *U.S. Hotelier Agrees to Buy Hospitality Software Firm From Chinese Owners Ordered to Sell by Trump*, WALL ST. J (Aug. 31, 2020), https://www.wsj.com/articles/u-s-hotelier-agrees-to-buy-hospitality-software-firmfrom-chinese-owners-ordered-to-sell-by-trump-11598853600.

78. *See* PATIENTSLIKEME, https://www.patientslikeme.com/about (last visited Aug. 21, 2021) (claiming to have over 830,000 users sharing stories to improve the lives of other patients through knowledge derived from the platform's shared real-world experiences).

79. *See* GRINDR, https://www.grindr.com/about/ (last visited Aug. 21, 2021) (claiming to be the largest LGBTQ app with "millions of daily users . . . in every corner of the planet").

80. *See The Future Is Bright for StayNTouch, Backed by New Owners MCR Investors and $10M Investment*, STAYNTOUCH (Aug. 31, 2020), https://www.stayntouch.com/news/stayntouch-new-owners-mcr-investors.

A. LEGAL ISSUES OF THE BAN: IEEPA'S STATUTORY LIMITATIONS

1. Unusual and Extraordinary Threat

IEEPA's emergency power can be invoked only when an "unusual and extraordinary threat" exists. It is worth discussing whether the apps indeed posed an unusual and extraordinary threat that justified the use of IEEPA. Congress only described that such a threat must have its source "in whole or substantial part outside the United States"[81] but did not specify what qualifies as "unusual and extraordinary." Notably, courts have not discussed what "national emergency" entails under IEEPA,[82] and the statute does not require the president to prove that such a threat exists.[83] Thus, it may be helpful to look at the plain meaning of the terms and examine the recent uses of IEEPA to draw a line for unusual and extraordinary threats.[84]

According to Black's Law Dictionary, "unusual" means something "extraordinary" or "abnormal,"[85] while "extraordinary" means something beyond common, involving an unforeseeable incident, or something "[e]mployed for an exceptional purpose."[86] Read together, these words depict a unique set of unforeseeable circumstances, and the use of IEEPA is reserved for that exceptional purpose.[87] The question then becomes whether either app constituted an exceptional, unforeseeable risk that warranted the use of emergency power under IEEPA.

In TikTok's case, ByteDance's acts of acquiring Musical.ly in 2017 and merging Musical.ly into TikTok,[88] without more, would not seem sufficient to trigger IEEPA, as foreign investment has become relatively common in the global economy.[89] Instead, the focus should be on the two issues raised in the EO: the government's concerns about (1) data collection and (2) the CCP's censorship and disinformation campaigns.[90]

---

81. 50 U.S.C. § 1701(a).

82. *See* Marcus Noland et al., *Assessing Trade Agendas in the US Presidential Campaign*, PETERSON INST. INT'L ECON. (Sept. 2016), https://www.piie.com/publications/piie-briefings/assessing-trade-agendas-us-presidential-campaign (last visited Aug. 22, 2021) (describing that while IEEPA is supposed to be exercised only during an unusual and extraordinary threat, courts have never questioned presidential declarations of a "national emergency," so the precedent seemingly gave President Trump a free hand).

83. Boyle, *Checking the President's Sanctions Powers*, *supra* note 32, at 22.

84. *See* Allman, *supra* note 46, at 315–16.

85. *Unusual*, BLACK'S LAW DICTIONARY (11th ed. 2019).

86. *Extraordinary*, BLACK'S LAW DICTIONARY (11th ed. 2019).

87. Allman, *supra* note 46, at 317.

88. Musical.ly was a China-based video-sharing platform with limited assets in the United States. It was acquired in November 2017 by ByteDance, which already owned TikTok, a Muscial.ly equivalent (in China, TikTok is called Douyin). In August 2018, TikTok absorbed Musical.ly, automatically migrating all Musical.ly accounts to TikTok. *See* TikTok Complaint, *supra* note 17, at 15; Rebecca Jennings, *TikTok, Explained*, VOX (updated July 12, 2019), https://www.vox.com/culture/2018/12/10/18129126/tiktok-app-musically-meme-cringe.

89. *See* Allman, *supra* note 46, at 319.

90. TikTok EO, *supra* note 2.

i. The Threat of Data Collection

First, data security could be a legitimate concern, since Beijing's administration reportedly has certain control over private companies.[91] Even if companies promise not to provide user data to the government, according to the espionage and national intelligence laws in China, organizations and citizens are still obligated to assist and cooperate with national intelligence work.[92] Accordingly, when such a situation arises, companies likely cannot say no to the government.[93] However, from this perspective, arguably every Chinese-owned company with access to its U.S. customer data can be subject to the CCP's surveillance and can impair U.S. national security. Nevertheless, not every Chinese-owned app or company is forced to cease operation in America.[94] Thus, it is critical to explore under what circumstances the risks to personal data become exceptional and rise to national security levels that warrant government intervention.

a. The Number of Users

Some factors might include (1) the number of users as well as (2) the security vulnerabilities and type of data collected.[95] If the pervasiveness of the service is a defining factor that triggers government intervention, the scale and depth of the risk posed by the two apps, in particular WeChat, is distinguishable from Huawei's. Huawei intended to provide critical 5G equipment worldwide.[96] The Huawei ban might also make more sense when put in the context of the heavily regulated telecommunications industry. During World War I, the U.S. government seized foreign-owned radio

91. Arjun Kharpal, *Huawei Says It Would Never Hand data to China's Government—Experts Say It Wouldn't Have a Choice*, CNBC (Mar. 4, 2019), https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html (pointing out that Huawei would have no choice but to hand over network data to the Chinese government if asked for it, because China's National Intelligence Law and the Counter-Espionage Law require citizens and companies to assist and cooperate with national intelligence work).

92. *Id*. ("The 2014 Counter-Espionage law says that 'when the state security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals shall provide it truthfully and may not refuse.'").

93. *Id.*

94. For instance, Weibo is a popular Chinese-owned microblogging app that is still available for use and download in the United States. *See infra* notes 109–110 and accompanying text.

95. *See* Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021) (enumerating indicators of risk to consider such as "ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities"; "the scope and sensitivity of the data collected;" and "the number and sensitivity of the users" of the app).

96. Brian Fung, *How China's Huawei Took the Lead over U.S. Companies in 5G Technology*, WASH. POST (Apr. 11, 2019), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/ (noting that nearly no U.S. company manufactures the 5G technology's most critical components, so the country had to rely on foreign suppliers like Ericsson, Nokia, Huawei, and ZTE).

stations,[97] and Congress later enacted a statute limiting foreign stock ownership in a U.S. broadcast or common carrier licensee.[98] The U.S. government is often actively involved in the licensing industries considering the public interest they serve. In this context, it seems understandable that the Trump administration would forbid Huawei to be a part of the U.S. telecommunications supply chain.

TikTok and WeChat, on the other hand, are social media platforms. While TikTok boasts over 100 million active users in the United States, it may not be as pervasive as the 5G network—as 5G is estimated to be the leading mobile network technology by 2025, with more than 190 million connections in the United States.[99] WeChat's userbase in America is even smaller, with approximately 19 million daily active users as of August 2020.[100] It seems that neither app's influence is comparable to that of Huawei so as to constitute an equally significant threat to the country.

b. Security Vulnerabilities and the Type of Data Collected

If the userbase is not dispositive, other possible factors supporting government intervention might be certain security vulnerabilities within the apps or the type of data collected by TikTok and WeChat that would put the nation at risk. The Trump administration alleged that TikTok collects network activity information, such as location data and browsing histories.[101] As for WeChat, there was no specific allegation as to what kind of data is collected, but the government referenced a report in March 2019, when a Chinese database was found to contain billions of WeChat messages sent from users not only in China, but also in the United States and several other countries, which could be accessed by the CCP.[102] To be fair, most, if not all,

97. J. GREGORY SIDAK, FOREIGN INVESTMENT IN AMERICAN TELECOMMUNICATIONS, at 51–52 (1997).

98. *See generally* Communications Act of 1934 (codified as amended at 47 U.S.C. § 310(a), (b)); FED. COMM. COMM'N, *Foreign Ownership Rules and Policies for Common Carrier, Aeronautical En Route and Aeronautical Fixed Radio Station Licensees*, https://www.fcc.gov/general/foreign-ownership-rules-and-policies-common-carrier-aeronautical-en-route-and-aeronautical (last visited Aug. 21, 2021) (prohibiting foreign nationals from holding office in license companies and from owning more than 20% of stock in a broadcast, common carrier, or radio station licensee).

99. *The 5G Era in the US*, GSMA (2018), https://www.gsma.com/publicpolicy/wp-content/uploads/2018/03/The-5G-era-in-the-US.pdf (noting the forecast of 190 million connections has not counted in 5G-based fixed wireless).

100. *See* Krystal Hu, *WeChat U.S. ban cuts off users link to families in China*, REUTERS (Aug. 7, 2020), https://www.reuters.com/article/us-usa-tencent-holdings-wechat-ban-idINKCN253339.

101. TikTok EO, *supra* note 2 (stating TikTok captures vast swaths of information such as users' location data, browsing and search histories, which threatens to allow the CCP 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).

102. *See* WeChat EO, *supra* note 2; *see also* Emily Feng, *China Intercepts WeChat Texts from U.S. and Abroad, Researchers Say*, NPR (Aug. 29, 2019), https://www.npr.org/2019/08/29/

apps and searching engines collect vast swaths of data to optimize user experience, and the collection of location data, browsing histories, and chat messages is fairly common.[103] The app operators might claim that the data is necessary to provide communications service, as noted in their privacy policy, which is consented to by the users.[104] Several other communications services, such as Zoom, have also been found with security vulnerabilities that could pose risks to the users.[105] While several companies and even U.S. government agencies have discouraged employees from using Zoom, this videoconferencing service is still widely used by Americans, especially since the outbreak of the pandemic, and this widespread use could potentially affect data security on a large scale.[106]

If data collection from a foreign adversary is itself so extraordinary that it would trigger government intervention, other Chinese-owned services should have received the same treatment. The Trump administration had, in fact, attempted to ban several other Chinese apps in early 2021,[107] but the order, along with the TikTok-WeChat ban, was later revoked by the Biden Administration in June 2021.[108] Another curious case is Weibo, a Chinese-owned Twitter-like social media app[109] that is widely used in China and available in U.S. app stores.[110] In 2019, a data leak was reported when the

751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says (reporting that a Dutch researcher discovered a Chinese database storing over 3.7 billion WeChat messages tagged with a GPS location, over 19 million of which were sent from people outside China. They were mostly from the United States, Taiwan, South Korea and Australia, with the researcher noting that "the system resembles the global surveillance methods used by the U.S. National Security Agency").

103. *See generally Privacy & Terms*, GOOGLE, https://policies.google.com/privacy?hl=en-US (enumerating the vast information Google collects from its users).

104. *See, e.g.*, *Privacy Policy*, WECHAT, https://www.wechat.com/en/privacy_policy.html (storing chats temporarily in WeChat's server for the provision of communication service and collecting location data for location customization).

105. *New Zoom Vulnerability*, ROCKET IT (Apr. 27, 2021) https://rocketit.com/zoom-vulnerability-zero-day-security-update/ (reporting past vulnerabilities such as "Zoom Bomb" and a new vulnerability disclosed in April 2021 that could allow a cybercriminal to remotely access a victim's computer through Zoom).

106. *See* Brandon Vigliarolo, *Who Has Banned Zoom?* TECHREPUBLIC (Apr. 9, 2020), https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/ (noting that entities like Google and NASA have banned employees from using Zoom, and the New York City Department of Education has banned teachers from using Zoom and has encouraged them to use Microsoft Teams instead).

107. Exec. Order No. 13971, 86 Fed. Reg. 1250 (Jan. 5, 2021) (attempting to ban a few more Chinese apps including Alipay, CamScanner, Tencent QQ, WeChat Pay, and WPS Office).

108. Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021) (revoking three EOs: the TikTok and WeChat EOs issued on August 6, 2021, and the EO issued on January 5, 2021 banning other Chinese-owned apps).

109. Created in August 2009 by Chinese technology company Sina Corporation, Weibo is China's most popular microblogging site with 430 million active users per month as of 2018. Yuan Ren, *Know Your Chinese Social Media*, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/fashion/china-social-media-weibo-wechat.html.

110. *See, e.g.*, *Weibo*, APP STORE, https://apps.apple.com/us/app/weibo/id350962117 (last visited Nov. 7, 2021); *Weibo*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.

data of Weibo's 500 million users worldwide had been hacked and leaked to the dark web.[111] Although the leaked data reportedly contained no passwords or payment information, it could still make Weibo users' data available to hackers, including their full names and phone numbers.[112] Similar to WeChat, Weibo does not have a big presence in America,[113] but such security risks could still be detrimental to users in the country.[114] Nevertheless, as of November 2021, people can still download and use Weibo in the United States.

ii. The Threat of Censorship and Disinformation

Regarding the government's second claim about censorship and disinformation concerns, it is unlikely the two apps are the only platforms that are censored or swamped by disinformation. It is also doubtful whether categorically banning the apps can effectively solve the problem. The TikTok EO asserts that TikTok's videos spread conspiracy theories about the origins of COVID-19 as an example that the app may be used for disinformation campaigns that benefit the CCP.[115] However, disinformation is hardly uncommon on social media platforms. Big social media sites like Facebook and Twitter have also given users a platform to spread false and malicious content about the virus.[116] Despite Facebook and Twitter's efforts to fact-check and direct users to reliable sources, false information remains pervasive online.[117] One may argue that TikTok should likewise endeavor to minimize the harm caused by disinformation, but there is no existing law requiring an online platform like TikTok to do so.[118] Moreover, when it comes to censorship, Weibo is also said to be heavily censored and often used

weico.international&hl=en (last visited Nov. 7, 2021) (showing that Weibo is downloadable from both Apple's and Google's app stores).

111. Scott Ikeda, *Data of 538 Million Weibo Users Is Available on the Dark Web for Only $250*, CPO MAGAZINE (Apr. 3, 2020), https://www.cpomagazine.com/cyber-security/data-of-538-million-weibo-users-is-available-on-the-dark-web-for-only-250/.

112. *Id.* (reporting over 500 million users' names and 172 million users' phone numbers were held for sale).

113. *All You Need to Know About Weibo*, APARTNERSHIP (Apr. 18, 2019), https://apartnership.com/all-about-weibo/ (describing that Weibo had approximately 2.5 million registered users in the United States as of 2018).

114. Ikeda, *supra* note 111.

115. TikTok EO, *supra* note 2.

116. *See, e.g.*, Sheera Frenkel et al., *Surge of Virus Misinformation Stumps Facebook and Twitter*, N.Y. TIMES (June 1, 2020), https://www.nytimes.com/2020/03/08/technology/coronavirus-misinformation-social-media.html (describing that a few Facebook posts falsely stated that Taiwan concealed many infections of COVID-19, which some suspected to be China's doing to undermine Taiwan's sovereignty).

117. *See id.*

118. *See, e.g.*, Daisuke Wakabayashi, *Legal Shield for Social Media Is Targeted by Trump*, N.Y. TIMES (May 28, 2020), https://nyti.ms/2Bb7fS4 (noting that Section 230 of the Communications Decency Act shields websites from liability for content created by users; sites can moderate content by setting their own rules for what is and what is not allowed without being liable for everything posted by visitors).

as a political instrument to foster CCP's public image,[119] but the ban did not target this app.

If the threat of data breach and disinformation on social media is so unusual and extraordinary, other platforms that pose similar risks, like Weibo, should likewise be subject to scrutiny. Considering a recent incident related to TikTok videos that allegedly impacted Trump's campaign efforts in the 2020 U.S. presidential election[120] and how the U.S.-China tension escalated since the outbreak of COVID-19,[121] it is hard to ignore the possibility that the TikTok-WeChat ban was more of a political action, as opposed to merely an action to counter a national security threat.

2. The Informational Materials Exception

Even assuming an "unusual and extraordinary threat" exists, the presidential power under IEEPA is not unbounded. The statute expressly bars the president from regulating or prohibiting, directly or indirectly, (1) the importation or exportation of any "information or informational materials" or (2) "personal communication[s]" that do not involve a transfer of anything of value.[122] Due to these limitations, TikTok,[123] TikTok's users,[124] and WeChat's users each brought a lawsuit to enjoin the ban.[125] Had they not been enjoined, the bans would have removed the apps from app stores, preventing U.S. users from downloading or updating the apps and ultimately restricting users from using the apps.[126]

119. *See, e.g.*, *China Covid-19: How State Media and Censorship Took on Coronavirus*, BBC (Dec. 29, 2020), https://www.bbc.com/news/world-asia-china-55355401 (noting that media reports questioning the Chinese government's handling of the COVID-19 pandemic were stifled on Weibo and that posts supporting and mourning the death of a whistleblower doctor had been periodically wiped); *see also* Ren, *supra* note 109 (noting that little political content on Weibo is user-generated because censors quickly remove anything that is deemed sensitive).

120. *See, e.g.*, Taylor Lorenz et al., *TikTok Teens and K-Pop Stans Say They Sank Trump Rally*, N.Y. TIMES (Sept. 14, 2020) https://www.nytimes.com/2020/06/21/style/tiktok-trump-rally-tulsa.html (reporting that TikTok users claimed to have "pranked" President Trump's rally in Tulsa in June 2020 by registering tickets for the campaign and encouraging TikTok viewers to do the same and not show up, resulting in the planned events outside the rally being cancelled as the anticipated one-million-crowd did not materialize).

121. *See* Weizhen Tan, *US-China Relations at a Low as 'Blame-Shifting' Sets Back War Against Virus*, CNBC (Apr. 21, 2020), https://www.cnbc.com/2020/04/22/coronavirus-trump-blames-china-virus-impact-on-trade-war.html.

122. 50 U.S.C. §§ 1702(b)(1) & (b)(3).

123. TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 100 (D.D.C. 2020), *appeal dismissed sub nom.* TikTok Inc. v. Biden, No. 20-5381, 2021 WL 3082803 (D.C. Cir. July 14, 2021).

124. Marland v. Trump, 498 F. Supp. 3d 624, 632 (E.D. Pa. 2020).

125. U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 916 (N.D. Cal. 2020).

126. The Department of Commerce outlined the types of transactions prohibited by the EOs, including "any provision of service to distribute or maintain the WeChat or TikTok mobile applications, constituent code, or application updates through an online mobile application store in the U.S." Press Release, Wilbur Ross, U.S. Dep't of Commerce, Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States (Sept. 18, 2020), https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.

In *TikTok Inc. v. Trump*, TikTok claimed that the prohibitions were impermissible because the use of the app falls within IEEPA's informational materials exception.[127] Under IEEPA, the president may not regulate the importation or exportation of informational materials "regardless of format or medium of transmission," and "whether commercial or otherwise."[128] Such materials include publications, films, photographs, artworks, and news wire feeds.[129] TikTok contended that over 100 million Americans use the app to share their films, photographs, and news, which constitute informational materials, with users across the globe.[130]

The D.C. court in *TikTok* granted a preliminary injunction, finding that TikTok had demonstrated a likelihood of success on this claim because TikTok is a medium transmitting informational materials.[131] The court explained that the government's goals included "stopping the exportation of data (which the government itself defines as 'text, images, video, and audio') to China and stopping the importation of propaganda into the United States."[132] Since these objects constitute informational materials within IEEPA's definition, the ban sought to control what is prohibited by the statute.[133] Moreover, the court found that by shutting down the app, the executive branch sought to achieve a secondary goal of stopping CCP propaganda from spreading in the United States, which is still at minimum indirectly regulating the exchange of texts, images, and videos via the app.[134]

The Eastern District of Pennsylvania in *Marland v. Trump* similarly granted an injunction, enjoining the entirety of the TikTok EO because the plaintiffs (a group of TikTok users) showed a likelihood of success in their argument that the prohibitions violated IEEPA.[135] The government tried to defend its position by arguing that the informational materials exception does not apply to materials that are "not fully created and in existence at the date of the transactions,"[136] and since most TikTok videos are not created prior to transactions, they can be regulated.[137] The court rejected this argument,

127. *TikTok*, 507 F. Supp. 3d at 108.
128. 50 U.S.C. § 1702(b)(3).
129. *Id.*
130. *TikTok*, 507 F. Supp. 3d at 108.
131. *Id*. at 112–15.
132. *Id*. at 105–09.
133. *Id*. at 108 (explaining that pictures, art, and films are included in the statutory definition itself).
134. *Id*. at 103.
135. Marland v. Trump, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020).
136. 31 C.F.R. § 560.210(c)(2) (2020); *see also Marland*, 498 F. Supp. 3d at 639–40 (citing a Third Circuit case, *United States v. Amirnazmi*, 645 F.3d 564, which gave deference to the Office of Foreign Asset Control's interpretation that this exception does not include "transactions related to information or informational materials not fully created and in existence at the date of the transactions").
137. TikTok countered users can film and design content outside of TikTok's system (e.g., on their phone or other apps) and post on TikTok later. When users share such pre-made videos, those

reasoning that Congress's purpose in creating this exception was to "facilitat[e] transactions and activities incident to the flow of informational materials," so as to ensure the "robust exchange of informational materials."[138] The focus should not be on whether those materials existed prior to the transactions, but why Congress chose to protect such activities.[139] Since the prohibitions would have the effect of shutting down a platform used by 100 million individuals[140] as a means to exchange information, the EO presented a threat to the "robust exchange of informational materials" and therefore fell under the informational materials exception.[141]

3. The Personal Communications Exception

In addition to the informational materials limitation, IEEPA prohibits the president from regulating personal communications that do not involve a transfer of anything of value.[142] While some transactions of the two apps have economic value, the apps' users argued that many videos, comments, and private messages on the two apps are merely communications with no economic value.[143] In *TikTok*, the government countered that regardless of their value to the creators, these communications eventually benefit TikTok as a platform and thus should not be exempt from regulation.[144] However, the court found that every communications service provider gets some value from a user's presence on its platform.[145] The value of a social media app relies heavily on the users' presence on its network, which attracts more people to the site, expanding the userbase. The court reasoned that the government's broad interpretation would make all communications services fall under this category, which essentially renders the entire personal communications exception meaningless.[146] This was not likely Congress's intent when it inserted this limitation.[147] Thus, the phrase "anything of value" should refer to the transfer of value "between participants in a personal communication itself,"[148] such as when a TikTok user sends a gift to a TikTok

videos are arguably "fully created and in existence" before they reach TikTok's platform. *Marland*, 498 F. Supp. 3d at 639; *Tiktok*, 490 F. Supp. 3d at 82 n.2.

138. *Marland*, 498 F. Supp. 3d at 640 (quoting *Amirnazmi*, 645 F.3d at 586–87).

139. *Id.*

140. *Id.* at 640–41 (noting that TikTok is used by over 100 million individuals in the United States, and at least 50 million of these U.S. users use the app daily).

141. *Id.*

142. 50 U.S.C. § 1702(b)(1).

143. TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 107 (D.D.C. 2020), *appeal dismissed sub nom.* TikTok Inc. v. Biden, No. 20-5381, 2021 WL 3082803 (D.C. Cir. July 14, 2021); *see also* Amended Complaint for Declaratory and Injunctive Relief at 31, U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912 (N.D. Cal. 2020) (claiming that plaintiffs use WeChat for personal communications that do not involve a transfer of anything of value).

144. *TikTok*, 507 F. Supp. 3d at 107.

145. *Id.* at 107–08.

146. *Id.* at 108.

147. *Id.*

148. *Id.*

star during a live stream. However, the gifting function is not available to those who are under 18 years old,[149] and not all TikTok users send gifts when they watch a TikTok live stream. Since not all communications on TikTok involve a transfer of value between the participants, the TikTok EO was enjoined.[150]

On the other hand, unlike in *TikTok*, the Northern District of California in *U.S. WeChat Users All v. Trump* reasoned that even if the app were to be removed from app stores, current users could keep using it to communicate with others, so the WeChat EO hardly restricted personal communications.[151] However, this view fails to consider that if the EOs had been effective and the apps had been removed by September 2020, those who did not install the apps would no longer have access to the apps.[152] Current users would not be able to update their apps, which could exacerbate the security risks to users.[153] Eventually, users might not be able to use any new functions or the app entirely in the near future.[154] In this sense, the administration still regulates, at least indirectly, personal communications involving nothing of economic value.

B. ECONOMIC IMPLICATIONS OF THE TIKTOK-WECHAT BAN

In addition to the legal problems, the TikTok-WeChat ban has created significant economic costs. One obvious impact is on the apps' parent companies. On August 14, 2020, the Trump administration issued a subsequent order mandating that ByteDance either sell or spin off its U.S. business within a limited timeframe.[155] Unlike Grindr, which was reportedly granted more than one year to complete its divestment,[156] TikTok was only

149. *Live Gifting*, TIKTOK, https://www.tiktok.com/creators/creator-portal/en-us/getting-paid-to-create/live-gifting/ (last visited Oct. 31, 2021).

150. *TikTok*, 507 F. Supp. 3d at 108.

151. U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 926–28 (N.D. Cal. 2020) (granting the WeChat Users Alliance's injunctive relief on First Amendment grounds but finding that the personal communication challenge was unlikely to succeed because the record and arguments did not show that the elimination of support for the app, like upgrades and throttling internet services, prohibited personal communications).

152. *See TikTok*, 507 F. Supp. 3d 92, 106.

153. In a subsequent order denying the government's motion to stay, the court mentioned an expert opinion noting that "[b]anning WeChat downloads is dangerous because it increases security risks to users: software needs updates to fix bugs, and if bugs are not fixed, WeChat users' devices and data are subject to attack." U.S. WeChat Users All. v. Trump, No. 20-CV-05910-LB, 2020 WL 6891820, at *5 (N.D. Cal. Nov. 24, 2020).

154. *TikTok*, 507 F. Supp. 3d 92, 109–22 (explaining that the TikTok EO and the prohibitions will have the intended effect of stopping U.S. users from communicating on TikTok since the ultimate purpose of those prohibitions is to protect national security by preventing China from accessing data on TikTok).

155. Presidential Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 14, 2020) (mandating ByteDance to divest within 90 days of the order).

156. *See* Peters, *supra* note 71 (noting that CFIUS reportedly informed Kunlun of the national security risk in March 2019 and set a deadline to sell Grindr by June 2020).

given 112 days in total to finalize a deal.[157] While TikTok located Oracle and Wal-Mart as its potential buyers,[158] this was a rather limited timeframe for a big company like TikTok to adequately evaluate its options, finalize the terms, and get approval from the government.[159]

Even if the government had officially greenlit TikTok's deal with Oracle, the rushed deadline and wide media coverage of the TikTok ban still negatively affected TikTok's stakeholders and certain businesses associated with ByteDance. For example, the stock of a cloud services provider, Fastly, plunged 37% after the August 6th EO because ByteDance had been its largest customer.[160] Moreover, the ban could have caused several TikTok creators to lose their influence and affected their livelihood, as the uncertainty of the app's future drove some fans to other platforms and social media users often do not return to the platforms they abandon.[161]

Further, businesses that use WeChat as a communication tool might also have been negatively impacted. For instance, many Chinese restaurants in the United States use WeChat to advertise and communicate with their customers—most of them are of Chinese descent.[162] Since 2020, restaurants

157. The original order specified a 90-day period to complete the divestment, but the government granted TikTok's request to extend the deadline to November 27, 2020, and again to December 4, 2020, to finalize the deal. *See TikTok,* 507 F. Supp. 3d 92, 101.

158. Brian Fung, *Trump Says He Has Approved a Deal for Purchase of TikTok*, CNN (Sept. 21, 2020), https://edition.cnn.com/2020/09/19/tech/donald-trump-tiktok-deal-approval/index.html.

159. Dave Simpson, *TikTok Asks DC Circuit to Block Trump's Divestment Order*, LAW360 (Nov. 10, 2020), https://www.law360.com/articles/1327990/tiktok-asks-dc-circuit-to-block-trump-s-divestment-order (mentioning ByteDance's request for extension to have more time to negotiate the final terms of a mitigation solution).

160. *See* Lee, *supra* note 21 ("ByteDance Ltd. pulled most of its TikTok traffic from the network of Fastly Inc., suggesting a crackdown by the Trump administration is forcing the Chinese technology giant to change its operations."); *see also* Ray, *supra* note 21 ("Due to the impacts of the uncertain geopolitical environment, usage of Fastly's platform by its . . . largest customer [ByteDance] did not meet expectations, resulting in a corresponding significant reduction in revenue from this customer.").

161. *See* TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 113 (D.D.C. 2020) (pointing out that the uncertainty in TikTok's future availability "has already driven, and will continue to drive, content creators and fans to other platforms"); McKenna Morgan, *Tik, Tok, Boom: How the U.S.'s Battle with TikTok Could Affect the Licensing Industry*, LICENSE GLOBAL (Sept. 25, 2020), https://www.licenseglobal.com/analysis/tik-tok-boom-how-uss-battle-tiktok-could-affect-licensing-industry.

162. Tony Lin, *What the Proposed Ban on WeChat Means for NYC Chinese Restaurants*, EATER N.Y. (Oct. 26, 2020), https://ny.eater.com/2020/10/26/21528905/wechat-chinese-restaurants-nyc-business-coronavirus.

have been struggling to survive during the COVID-19 pandemic.[163] WeChat has become a lifeline for them, as people rely more on apps like WeChat to order food and connect with people in the community.[164] Had the ban taken effect, restaurants would have lost their primary communication channel with customers, making it even harder to maintain their businesses.[165] While there might be other alternative apps, many people in Chinese communities still prefer WeChat to other communication apps.[166]

In addition to its direct impact on the stakeholders and users, a total ban on the apps might present obstacles to other U.S. corporations as well. Companies worried that the WeChat ban might undermine their competitiveness worldwide and especially in the Chinese market.[167] WeChat's prominence in Chinese communities is incomparable—it is a multifunctional app that serves for messaging, calling, mobile payment, and even conducting business all in one place.[168] Most importantly, a great majority of people in China use it for mobile payments.[169] Commentators have observed that it would be difficult for American companies to survive in this market without being able to use WeChat payments.[170]

While U.S. officials have claimed that American companies can still conduct business in China regardless of the ban,[171] China warned of its intention to retaliate against the Trump administration by issuing the "Regulations on Unreliable Entity List" (UEL) in September 2020.[172] Through the UEL, if China believes that a foreign entity's action would harm its national interests, the government can issue sanction-style designations

163. *See, e.g.*, Nikko Duren, *NYC Restaurant Closings*, INFATUATION (May 20, 2021), https://www.theinfatuation.com/new-york/features/nyc-restaurant-closings (providing a running list of all the restaurants in New York City that have closed during the pandemic).

164. Lin, *supra* note 162.

165. *Id.*

166. *Id.*

167. Jonathan Garber, *WeChat ban endangers US businesses in China*, FOX BUS. (Sept. 12, 2020), https://www.foxbusiness.com/markets/wechat-poses-looming-threat-for-us-businesses-in-china.

168. Kelly and Rauhala, *supra* note 5.

169. Garber, *supra* note 167 (noting that mobile payments made up approximately 83% of all purchases in China in 2018, with about 92% of the business split between WeChat and Alibaba's Alipay).

170. *Id.* (noting if customers could not use the WeChat payment method, companies like Nike would likely lose their business to rivals such as Adidas, which is based in Germany where such a ban does not exist. The WeChat ban might also cause companies domiciled outside the United States whose apps ride on the WeChat system to "stop using the app in fear of secondary sanctions.").

171. Jennifer Jacobs et al., *Trump Officials Say WeChat Ban Won't Keep Apple out of China*, L.A. TIMES (Aug. 21, 2020), https://www.latimes.com/business/technology/story/2020-08-21/trump-wechat-ban-apple-china.

172. *China Slams US 'Bullying,' Warns of Action over TikTok, WeChat*, AL JAZEERA (Sept. 19, 2020), https://www.aljazeera.com/economy/2020/9/19/china-slams-us-bullying-warns-of-action-over-tiktok-wechat.

against the entity.[173] Although China has not publicly named any entity, reports have found that the measures could be used against certain U.S. companies.[174] From this perspective, the U.S. government's intervention in private business may jeopardize the nation's economy and competitiveness in the global market.[175] In the long run, it is unclear whether the benefits of categorically banning the apps outweigh the costs brought on by this action.

III. PROPOSAL: FIRRMA AS A BETTER OPTION AND POSSIBLE REFORMS TO CFIUS FIRRMA

In light of the foregoing legal and economic problems, the executive branch should consider other options to address the risks posed by TikTok, WeChat, and other software that might arise in the future. A total ban of the services might do more harm than good. The following paragraphs propose that (1) in the existing framework, FIRRMA might be a better route for the U.S. government to deal with an entity whose foreign investment or ownership implicates a threat to national security, and (2) certain reforms to CFIUS's role and FIRRMA's framework might be helpful to better serve the interests of the country and affected parties.

A. FIRRMA AS A BETTER OPTION

FIRRMA may be a better option for several reasons. First, contrary to IEEPA's statutory limitations, FIRRMA provides clearer legal grounds for the executive to act upon a foreign entity involving a U.S. business that collects sensitive personal data that may be exploited in a manner that impairs national security.[176] As discussed earlier, the government has used this legal authority to regulate online platforms and software like Grindr, PatientsLikeMe, and StayNTouch that similarly implicated national security concerns.[177]

One may argue that unlike Grindr's user data involving sexual orientation and HIV status, the data collected by TikTok and WeChat is not necessarily sensitive and thus does not fall within FIRRMA's purview.

173. Michael Zhang and Reid Whitten, *Certainties and Uncertainties Under China's New Unreliable Entity List*, SHEPPARD MULLIN (Sept. 22, 2020), https://www.chinalawupdate.cn/2020/09/articles/global-trade/chinas-new-uel-unreliable-entity-list/.

174. AL JAZEERA, *supra* note 172 (noting that while China did not mention any specific entities, state-run tabloid Global Times reported the measures would target U.S. companies such as Apple, Cisco, and Qualcomm, while suspending purchases of Boeing airplanes).

175. McKinnon & Wei, *supra* note 18; Straub, *supra* note 22.

176. 50 U.S.C. § 4565(a)(4)(B)(iii)(III) (2012) (defining a covered transaction to include any investment "by a foreign person in any unaffiliated United States business that … maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security").

177. *See supra* notes 70–76 and accompanying text.

However, FIRRMA's subsequent implementing regulations define "sensitive personal data" to include ten categories of identifiable data[178] maintained or collected by a U.S. business that (i) "targets" to certain populations, such as U.S. military members and employees of certain federal agencies, (ii) "collects or maintains" such data on at least one million individuals, or (iii) has a "demonstrated business objective to maintain or collect" such data on more than one million individuals as part of its primary products or services.[179] The categories of data include financial data; health information; biometrics; "geolocation data collected using positioning systems, cell phone towers, or WiFi access points"; and "non-public electronic communications, including email, messaging, or chat communications," among other things.[180]

Based on this list, some of the data collected by the two apps could be deemed sensitive data. The data TikTok collects from its millions of users include payment information, location data, biometric identifiers, and messages, comments, and videos transmitted on the platform.[181] Under the regulation's definition, if these data elements are not encrypted or are capable of being used to distinguish or trace an individual's identity,[182] they would qualify as identifiable data and meet the criteria of sensitive personal data.[183] WeChat users also provide location data, chat communications, and even payment information to the app provider.[184] Accordingly, the data collected by the two apps arguably falls within the broad category of sensitive personal data. Unless the federal government enacts a data privacy law that specifically deals with this issue, currently the apps are likely within CFIUS's purview under FIRRMA.

178. 31 C.F.R. § 800.226 (2020) ("The term identifiable data means data that can be used to distinguish or trace an individual's identity, including through the use of any personal identifier . . . Identifiable data does not include encrypted data, unless the U.S. business that maintains or collects the encrypted data has the means to de-encrypt the data so as to distinguish or trace an individual's identity.").

179. 31 C.F.R. § 800.241(a)(1) (2020).

180. *Id.*

181. *Privacy Policy*, TIKTOK (June 2, 2021), https://www.tiktok.com/legal/privacy-policy-us?lang=en (describing that TikTok collects messages sent through their platform, geolocation information based on their users' SIM cards, IP addresses and even GPS, and biometric identifiers such as faceprints or voiceprints; users may also provide payment information such as credit card numbers to TikTok).

182. *Id.* (claiming to protect user data by encryption but does not "guarantee the security of [users'] information transmitted via the Platform" and thus users bear the risk of any transmission).

183. *See* 31 C.F.R. § 800.241(a)(1) (2020); *see also* 31 C.F.R. § 800.241(c)(1) (giving an example that when a corporation collects geolocation data for marketing purposes of greater than one million individuals, it meets the criteria of this section).

184. *See Privacy Policy*, WECHAT (Aug. 19, 2021), https://www.wechat.com/en/privacy_policy.html (listing data collected by WeChat including payment card information, location information derived from users' GPS, WiFi, and IP address, as well as chat messages—but the latter will be deleted permanently from WeChat's server within 3 hours of delivery to the recipient).

Second, even if the apps pose a threat that warrants government intervention, as opposed to a total ban, a divestiture will likely cause less harm and better serve the country's interests. The companies can negotiate a deal more quietly without too much public attention, which may better protect their stakeholders. In addition, the government in the past has not used FIRRMA to outright ban a service, especially after the transaction has been completed—it has either blocked the transaction before it occurred[185] or advised the owners to divest to enable the continued operations of the services.[186] While the statute authorizes the president to prohibit a transaction, it does not mention whether the government can prohibit the use of an existing service.[187] Similar to Grindr, PatientsLikeMe, and StayNTouch, the two apps TikTok and WeChat have been operating in this country before the government attempted to ban the apps. Unless the continued use of these two platforms posed greater risks than Grindr and the like, it appears that the Trump administration could have allowed the apps' operation in the country while communicating with their owners about risk mitigation measures.

Invoking IEEPA to categorically ban the apps does not necessarily serve the government's purpose either. The government's subsequent actions suggest that the U.S. administration was not entirely determined to force TikTok to cease operations in this country. On August 14, 2020, the executive branch provided an option for ByteDance to divest, which would allow TikTok's continued operations in the United States.[188] President Trump even gave his

185. *See, e.g.*, Presidential Order Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GmbH, 81 Fed. Reg. 88,607 (Dec. 2, 2016) (prohibiting Chinese investors' acquisition of Aixtron SE, a U.S semiconductor manufacturer, prior to the consummation of the transaction); Presidential Order Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited, 82 Fed. Reg. 43,665 (Sept. 13, 2017) (blocking the acquisition of Lattice Semiconductor by Chinese-controlled investor Canyon Bridge before the transaction).

186. *See, e.g.*, Farr & Levy, *supra* note 74 (describing that the Chinese owner divested from PatientsLikeMe but the platform was not said to be banned in the United States); Wang, *supra* note 70 (mentioning a few risk mitigation measures adopted by Kunlun and that no records showed Grindr was ever banned in the United States).

187. *See generally* 50 U.S.C. § 4565 (2012). FIRRMA also explicitly provides that the president may prohibit or suspend a transaction only when no law other than IEEPA or FIRRMA provides adequate and appropriate authority for the president to protect national security. 50 U.S.C. § 4565(d).

188. Presidential Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 14, 2020). This is the only EO that has not been revoked by the Biden Administration as of October 2021. *See* Chris Mills Rodrigo, *Rubio reiterates calls for Tik Tok ban after China's reported ownership stake*, THE HILL (Aug. 17, 2021), https://thehill.com/policy/568269-rubio-reiterates-calls-for-tik-tok-ban-after-chinas-reported-ownership-stake?rl=1.

blessing to Oracle's deal,[189] and the government extended the deadline twice for TikTok to finalize the deal.[190] On November 17, 2020, after the *TikTok* and *Marland* courts each granted an injunction, the Commerce Department announced that the ban pursuant to the TikTok EO on August 6, 2020 would not go into effect.[191] On June 9, 2021, President Biden announced a new EO, officially lifting the bans by revoking the WeChat and TikTok EOs and urging the federal government to "evaluate these threats through rigorous, evidence-based analysis."[192] The order further directed the Commerce Secretary to develop recommendations for how to protect Americans' sensitive personal data against foreign-adversary controlled systems.[193] While it is possible that CFIUS may still act against TikTok after reevaluation, especially given the Chinese government's reported stake in ByteDance revealed in August 2021,[194] the government's earlier actions suggest that a total ban was not needed in the first place when the risks were rather less imminent and yet to be fully evaluated. Therefore, instead of invoking IEEPA's emergency authority to ban the apps, the executive could have used other means such as FIRRMA to protect the nation in a less harmful and less costly manner.

B. POSSIBLE FUTURE REFORMS TO CFIUS AND FIRRMA

Although FIRRMA may better serve the parties' interests, it still has certain problems. As mentioned earlier, prior to the EO in August 2020, TikTok was already under CFIUS's review.[195] According to TikTok's complaint, CFIUS contacted ByteDance in 2019 about a possibility of reviewing ByteDance's acquisition of Musical.ly and initiated a formal review on June 15, 2020.[196] On July 30, the eve of its forty-five-day deadline,

189. *See* Debanjali Bose, *Oracle has struck a deal with TikTok to control its US operation. Take a look inside Trump's close relationship with Oracle cofounder, Larry Ellison*, BUS. INSIDER (Sept. 14, 2020), https://www.businessinsider.com/look-inside-president-trump-and-larry-ellisons-relationship-2020-8 (describing that President Trump said Oracle would certainly be a company that could handle TikTok's takeover and portraying Trump's close relationship with Oracle co-founder, Larry Ellison).

190. The original order specified a 90-day period, but the government extended the deadline to November 27, 2020, and again to December 4, 2020. TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 101 (D.D.C. 2020).

191. Notice of Preliminary Injunction Order, 85 Fed. Reg. 73,191 (Oct. 30, 2020) (informing the public of a preliminary injunction ordered by the court, preventing the Department of Commerce's implementation of the prohibitions).

192. Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021) (revoking three EOs: the TikTok and WeChat EOs issued on August 6, 2020, and the EO issued on January 5, 2021 that was meant to ban other Chinese apps).

193. *Id*; Chan, *supra* note 68.

194. Rodrigo, *supra* note 188 (reporting that ByteDance sold a 1% stake to a company owned by the Chinese government in April 2021, so a Congressman urged the Biden administration to renew the TikTok ban).

195. *See* TikTok Complaint, *supra* note 17, at 15.

196. *Id.*

CFIUS informed TikTok that it would have to divest because CFIUS had "identified national security risks arising from the [t]ransaction and that it has not identified mitigation measures that would address those risks."[197]

Although ByteDance claimed that it had provided voluminous information to assure CFIUS that U.S. user data was safeguarded, ByteDance said that CFIUS never explained why those safety measures were inadequate.[198] ByteDance stated that it also proposed various mitigation plans, including "spinning out TikTok's U.S. business to American investors."[199] ByteDance then notified CFIUS on July 30, 2020, that it had signed a nonbinding letter of intent with Microsoft, stating that Microsoft could serve as a trusted technology partner and acquire TikTok's U.S. business.[200] However, apparently, this proposal was not accepted, as President Trump later issued the EO in August 2020 banning the app.

Since CFIUS does not publicly publish its review process or rationale, it is unclear if or why CFIUS found TikTok's proposals unsatisfactory. Even if CFIUS was not satisfied with ByteDance's deal with Microsoft, given that the Trump administration seemed to support the Oracle deal, the security risk was not entirely immitigable. CFIUS could have communicated what conditions Microsoft, or a new buyer, must satisfy to mitigate that risk. In this way, the parties and the government could have prevented the subsequent ban and lawsuits.

CFIUS's reviewing process can still be improved, and Congress may consider further reforming the committee or adding oversight measures. For instance, it might be helpful to increase transparency and efficiency in the communication process between CFIUS and the parties. In *Ralls Corp. v. Comm. on Foreign Inv. in U.S.*, the D.C. Circuit noted that CFIUS or the president should at least inform the affected parties of its official action and give them access to the "unclassified evidence" that the government relied on.[201] Here, it is unclear whether TikTok was given such unclassified evidence of CFIUS's decision. Since there are no legal requirements to limit which documents can be deemed "classified,"[202] it is quite likely that the government would be unwilling to provide classified information

197. *Id.* at 17.
198. *Id.* at 16.
199. *Id.*
200. *Id.* at 17.
201. Importantly, the court also noted that CFIUS or the president need not provide classified information or disclose their thinking on sensitive questions related to national security when reviewing a covered transaction. Ralls Corp. v. Comm. on Foreign Inv. in U.S., 758 F.3d 296, 319-20 (D.C. Cir. 2014).
202. Jayden R. Barrington, *CFIUS Reform: Fear and FIRRMA, an Inefficient and Insufficient Expansion of Foreign Direct Investment Oversight*, 21 TRANSACTIONS: TENN. J. BUS. L. 77, 100 (2019)

especially when it is related to national security. However, if TikTok's description is accurate, ByteDance was already contemplating restructuring its U.S. business, which seems consistent with the government's goal in the divestment EO of August 14, 2020. When the parties had shown efforts to cooperate to serve the country's interest, CFIUS could well have acted in good faith to communicate those risk mitigation measures, rather than failing to respond to TikTok's proposals.[203] The government should consider means to promote CFIUS's efficiency and transparency in this regard.

Another problem that emerged from this case was the inconsistent timeframe afforded by the executive branch. While FIRRMA outlines CFIUS's screening timeline, the statute does not specify a timeframe for parties to respond to the executive's decision. Compared with ByteDance's 112 days, Grindr's former owner was reportedly given more than a year to complete divestiture.[204] Although presidents have ordered a thirty-day timeframe in the past, those were all scenarios where the transactions were blocked before they took place.[205] For a completed transaction, it seems reasonable to provide a longer period for parties to locate a suitable buyer to reduce economic impacts and for CFIUS to make sure the risk is properly mitigated. Thus, the government may consider specifying a standard procedure and timeline for CFIUS's post-review process or taking the time element into consideration when evaluating risk mitigation measures.

Additionally, even if TikTok and WeChat's data may qualify as sensitive personal data under FIRRMA, Congress should consider whether this is the result it intended. Despite the requirements such as "identifiable data" and "one million individuals" that were intended to limit the scope of CFIUS's review, more and more businesses will likely trigger these thresholds.[206] Scholars have observed that many businesses rely on data analysis to better understand customers' behavior patterns and preferences, and a technology startup with data collection as part of its primary services would likely have the business objective of surpassing one million customers,[207] which could subject it to CFIUS's review.[208] Moreover, since CFIUS can retroactively

203. TikTok Complaint, *supra* note 17, at 16 (noting that "CFIUS . . . effectively terminated formal communications with [ByteDance] well before the conclusion of the initial statutory review period" and that despite ByteDance's proposals to alleviate any national security concerns, CFIUS repeatedly refused to engage with ByteDance about CFIUS's concerns).

204. *See supra* note 156 and accompanying text.

205. *See, e.g.*, Presidential Order Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GmbH, 81 Fed. Reg. 88,607 (Dec. 2, 2016) (prohibiting a Chinese-invested company's acquisition of Aixtron SE prior to the consummation of the transaction).

206. Heath P. Tarbert, *Modernizing CFIUS*, 88 GEO. WASH. L. REV. 1477, 1518–19 (2020); *see also* Barrington, *supra* note 202, at 114–15 (noting that if an individual's financial data is considered sensitive and personal, then "most end-user service providers and merchants could be subject to CFIUS jurisdiction under FIR[R]MA because they collect individuals' credit card numbers").

207. Tarbert, *supra* note 206, at 1519.

208. *See* 31 C.F.R. § 800.241(a)(1) (2020).

review a completed acquisition,[209] this would create uncertainty for a corporation in the *ex-ante* assessment of whether to submit a declaration and when CFIUS's review might take place. Congress should consider revisiting the definition of sensitive personal data and evaluate whether the criteria still serve as meaningful thresholds to limit the scope of CFIUS's review.

In addition, even though FIRRMA is currently a better solution, CFIUS was not initially designed to tackle the increasingly complex data matters.[210] Given the increase in data privacy issues, asking CFIUS to take care of all data security matters can overburden CFIUS's ability to efficiently identify and mitigate national security issues in other types of foreign transactions.[211] To ensure CFIUS's efficiency and expertise, the legislature should consider finding another avenue—for instance, enacting a comprehensive federal data privacy law and establishing a federal agency focused on data protection—to properly address data security concerns.[212] Additionally, as noted in Biden's EO in June 2021, the government should set forth a clear set of criteria to evaluate security implications related to software apps and personal data,[213] both for the service providers' information and for Americans to be better informed of the risks to their data.

Lastly, although IEEPA and FIRRMA both allow the executive branch to address national security concerns posed by foreign entities, the statutes do not explain whether these two statutes can be used interchangeably. Nor does IEEPA mention whether the president can invoke the emergency powers if the risk is immitigable and less urgent. Since the two frameworks have different impacts and were intended to be used differently,[214] Congress may consider revisiting the statutes to clarify the relationship between the two frameworks to avoid potential abuse of executive power.

209. *See* Barrington, *supra* note 202, at 96.

210. *Id.* at 115–16.

211. *Id.* at 111 ("Ultimately, the incomplete structure of data protection law in the United States likely negates the potential benefits of this expansion. . . . The increase in transactions CFIUS would need to review as a result of this provision will likely burden the Committee's ability to efficiently identify national security issues involved in other transactions.").

212. *See, e.g.*, Nivedita Sriram, *Dating Data: LGBT Dating Apps, Data Privacy, And Data Security*, U. ILL. J.L. TECH. & POL'Y 507, 524–28 (2020) (proposing to implement a model like Europe's General Data Protection Regulation (GDPR) and create a federal agency that handles issues related to technological privacy and security because while the Federal Trade Committee has chief authority over privacy issues, it only steps in to protect consumers when a company has already violated its privacy policy. Apparently, "[t]here are clear gaps in federal protections of individual privacy and security rights that need to be addressed in a uniform, proactive, and clear manner").

213. Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (2021) (listing potential indicators of risk relating to connected software applications such as: "ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities"; and "use of the connected software application to conduct surveillance that enables espionage").

214. FIRRMA does not mention the term "national emergency," while IEEPA is meant to address urgent matters. *See generally* 50 U.S.C. §§1701-1702; 50 U.S.C. § 4565.

Despite all these problems, FIRRMA is by far the better solution to deal with data security issues posed by a social media app. IEEPA and FIRRMA were designed for different purposes: under FIRRMA, CFIUS's sole focus is on national security issues related to foreign investment, while IEEPA was designed to address an urgent situation where an unusual and extraordinary threat would impair U.S. national security. Unlike IEEPA's lack of criteria and definition of the term "national emergency," FIRRMA provides a list of factors to consider when evaluating the risks to national security.[215] Additionally, IEEPA's limitations on personal communications and informational materials make it unsuitable to regulate a social media app. In contrast, through the passage of FIRRMA, Congress specifically expanded CFIUS's jurisdiction over transactions involving critical technology, critical infrastructure, and sensitive personal data. Nowadays, technological advancements further complicate information security and privacy matters. Scholars have been concerned about the lack of substantial checks on presidents' use of IEEPA,[216] which makes it less ideal to tackle the increasingly complex data privacy issues that might need more rigorous analysis and input from professionals. Thus, the multiagency CFIUS, acting through FIRRMA's clearer statutory framework, is better suited to review foreign investment in critical technology industries and foreign entities' access to American's personal data that raise national security concerns.

CONCLUSION

In conclusion, in light of the legal and economic issues presented by the TikTok and WeChat bans, moving forward, the executive branch should consider using other means to deal with foreign entities that pose a similar threat to national security and data security. Given IEEPA's statutory constraints on personal communications and informational materials, as well as the ambiguous term "unusual and extraordinary threat," IEEPA is not the best tool to regulate a foreign entity's investment in critical technology industries or access to Americans' personal data. In contrast, FIRRMA provides clearer legal grounds for the government to act upon foreign entities whose collection of data may be exploited in a manner that would impair U.S. national security. Additionally, banning a service comes at a cost to the country and might not necessarily solve the data security problem. By invoking FIRRMA and acting through CFIUS, the government could similarly achieve its goals of mitigating the risks in a less harmful way. While CFIUS has certain shortcomings that would need further reforms or

215. 50 U.S.C. §§ 4565(d)(5), 4565(f).

216. Boyle, *Checking the President's Sanctions Powers*, *supra* note 32, at 3, 17 (noting the lack of congressional oversight on the president's use of IEEPA—it is difficult for Congress to muster a two-third majority to veto a national emergency declared by the president, and the president's consultations with Congress are often not regular and not comprehensive).

amendments, CFIUS's review process is by far a better option in the existing legal framework to serve the country's interest.

Ru Hochen[*]

* B.A., National Taiwan University, 2014; J.D. Candidate, Brooklyn Law School, 2022. I would like to thank Marissa Brown, Daniel Finnegan, Michelle Verkhoglaz, and the entire staff of the Brooklyn Journal of Corporate, Financial & Commercial Law for their thorough reviews throughout the editing process. I sincerely appreciated all professors who provided insightful and valuable feedback that helped me refine this Note. Lastly, thank you to my family and friends who listened to me ramble on about this topic and for their constant support.