POV: BALANCING FOREIGN ACTIVITY AND NATIONAL SECURITY THROUGH THE LENS OF TIKTOK

Soha AbdurRahman[*]

TABLE OF CONTENTS

I. INTRODUCTION

As 2020 took a turn with a global pandemic, millions of people flocked to TikTok to relieve their boredom.[1] TikTok is a Chinese-owned social media application that houses self-made, short-form videos varying across genres.[2] It is the first Chinese-owned app to gain a foothold in the United States, with downloads reaching over 2.8 billion as of mid-2021.[3] It is also the first Chinese application to match American social media platforms, such as Instagram and

* J.D. Candidate, University of Illinois College of Law Class of 2022. I would like to thank Professor Keenan and the JLTP editors for their guidance in creating this Note. I would also like to thank my family for their immeasurable support over the years. Lastly, I want to thank all my friends and mentors for their encouragement and advice during the writing process of this Note.

1. Robert Chesney, *TikTok and the Law: A Primer (In Case You Need to Explain Things to Your Teenager)*, LAWFARE (Aug. 2, 2020, 4:07 PM), https://www.lawfareblog.com/tiktok-and-law-primer-case-you-need-explain-things-your-teenager.

2. *Id*.

3. *TikTok by the Numbers: Stats, Demographics & Fun Facts*, OMNICORE, https://www.omnicoreagency.com/tiktok-statistics (Jan. 7, 2021).

YouTube, to become the second most popular social media app.[4] TikTok is owned by ByteDance, a Chinese tech company.[5] ByteDance acquired the American app Musical.ly, a lip-syncing video platform developed by Chinese developers for American audiences, in 2017 and merged it with TikTok, leading to the success of the app today.[6]

But as the app continues to grow in popularity, not everyone has hopped on board the viral application. Countries around the world have suspected TikTok as an intelligence-gathering app for the Chinese government.[7] TikTok distinguishes itself from most apps by curating videos for users based on their interests.[8] To accomplish this, TikTok collects vast amounts of data to curate user preference.[9] In its default setting, the app collects data ranging from location to IP address information.[10] If users opt-in, TikTok can also collect personal and payment information.[11] More recently, the app updated its privacy policy to allow the possible collection of user biometric data.[12] This vast data collection has raised concerns that China could access this data and use it for surveillance purposes.[13]

TikTok also has vulnerabilities outside China's data collection. TikTok is a prime space for hackers to gather personal information from users and take control of user accounts.[14] These vulnerabilities are attributed to the company's focus on growth rather than enhancing its security.[15] Concerns over TikTok's data collection have led several branches of the United States government to bar their employees from hosting the application on government devices.[16] Outside of the government, companies such as Wells Fargo have banned TikTok on company devices.[17]

In response to the increased concerns, the United States has contemplated banning or regulating the sale of TikTok, a move that would go against its

4. *Tiktok Beats Instagram to Become the Second Most Popular Social Media App for US Teens*, HT TECH (Oct. 8, 2020, 9:37 AM), https://tech.hindustantimes.com/tech/news/tiktok-beats-instagram-to-become-the-second-most-popular-social-media-app-for-us-teens-71602129774077.html.

5. Chesney, *supra* note 1.

6. Ronen Bergman et al., *Major TikTok Security Flaws Found*, N.Y. TIMES (Aug. 7, 2020), https://www.nytimes.com/ 2020/01/08/technology/tiktok-security-flaws.html.

7. Queenie Wong et al., *The Tiktok Saga: Everything You Need to Know*, CNET (Sept. 18, 2020, 7:11 AM), https://www.cnet.com/news/the-tiktok-saga-everything-you-need-to-know.

8. Robert McMillan et al., *TikTok User Data: What Does the App Collect and Why Are U.S. Authorities Concerned?*, WALL ST. J. (July 7, 2020), https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084.

9. Eugene Wei, *TikTok and the Sorting Hat*, REMAINS OF THE DAY (Aug. 4, 2020), https://www.eugenewei.com/blog/2020/8/3/tiktok-and-the-sorting-hat.

10. McMillan et al., *supra* note 8.

11. *Id*.

12. Sarah Perez, *TikTok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints'*, TECHCRUNCH (June 3, 2021, 5:57 PM), https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints.

13. Chesney, *supra* note 1.

14. Bergman et al., *supra* note 6.

15. *Id*.

16. *Id*.

17. Louise Matsakis, *Does TikTok Really Pose a Risk to US National Security?*, WIRED (July 17, 2020, 3:10 PM), https://www.wired.com/story/tiktok-ban-us-national-security-risk.

traditional open-door policy regarding foreign activity.[18] Safeguards such as the Committee on Foreign Investment in the United States (CFIUS) and the International Emergency Economic Powers Act (IEEPA) have allowed foreign activity to flourish with limited regulation. But with the arrival of TikTok and other similar foreign applications such as China's Grindr and WeChat and Russia's FaceApp,[19] the United States intends to increase restrictions on foreign activity within the country.[20]

Nonetheless, TikTok is the application that has become a proxy for countries to clash in the realm of foreign investment and tech development. To combat security concerns, the United States has attempted to force a sale or implement a ban on TikTok.[21] However, either approach leads to ramifications for the United States on a domestic and international front. Additionally, either response would be ineffective to mitigate the actual problem regarding national security while balancing the benefits of foreign activity. Rather, it is necessary to look to examples set by others, such as the European Union (EU), to address national security concerns that arise with applications like TikTok without risking the benefits of foreign activity.

To solve the precarious balance of national security and foreign activity, this Note argues that the United States, or more specifically CFIUS, needs to revise its approach towards reviewing foreign activity. By placing a rigorous and clear, but non-discriminatory, process in place, CFIUS can carve out a transparent process to reap the benefits of foreign activity within the country, while mitigating the security concerns that may arise due to the presence of such activity. Additionally, the United States should adopt clear internal guidelines, like the GDPR, to help guide foreign tech activity regarding data privacy, the biggest cause of concern for the United States.[22]

Part II of this Note documents the evolution of foreign activity within the United States and the country's response to the growing concern of national security regarding such activity. Part III analyzes the implications of a TikTok ban or sale on a domestic and international stage. It also analyzes the effectiveness of current U.S. and EU measures to regulate these issues. Part IV recommends CFIUS modify and clarify its regulation process and advises the implementation of internal statutory protections to mitigate security concerns but balance the influx of foreign activity.

18. Jayden R. Barrington, *CFIUS Reform: Fear And FIRRMA, An Inefficient and Insufficient Expansion of Foreign Direct Investment Oversight*, 21 TRANSACTIONS: TN. J. BUS. L. 77, 81 (2019).

19. Corey Nachreiner, *In Defense of Foreign-Based Apps, Part One*, FORBES (July 10, 2020, 8:50 AM), https://www.forbes.com/sites/forbestechcouncil/2020/07/10/in-defense-of-foreign-based-apps-part-one/?sh=60b8ba02fbfc.

20. Wong et al., *supra* note 7.

21. *Id*.

22. Bergman et al., *supra* note 6.

II. THE EVOLUTION OF THE UNITED STATES RESPONSE TO FOREIGN ACTIVITY

A. FDI, Technology, and China

In an increasingly global economy, the United States has benefitted from foreign activity flowing into the country. One major foreign activity within the United States is foreign direct investment (FDI).[23] The United States has long been a top-ranked destination for FDI.[24] FDI plays a big role in American economic prosperity and is used as a promoter of economic growth.[25] Inbound FDI has expanded domestic manufacturing, as seen with the $750 million expansion of the BMW American plant in South Carolina.[26] Inbound FDI has also provided for over 12 million jobs, or about 8.5% of the labor force, as of 2019.[27] FDI is a great investment tool between the United States and other economies due to its stability and longevity.[28] It allows for transferring of important skills and ideas between countries.[29]

However, there are security concerns tied with FDI. For one, countries too dependent on FDI can have FDI leveraged in political negotiations.[30] This is partly why unregulated FDI is opposed strongly—foreign influence and control can affect major sectors of a country.[31] For example, foreign control of American businesses affects control of American intellectual property.[32] The United States is the largest market for investments in private artificial intelligence (AI) companies.[33] One expert estimates that this industry attracted nearly $25.2 billion in investments in 2019.[34] This amount does not account for undisclosed investments.[35] Investments in this field are dominated by domestic and international private firms such as Google and Chinese-owned Baidu.[36] While domestic investments have grown, Chinese investment in the United States has grown in recent years from $2 billion in 2005 to over $14.9 billion in 2015.[37] The invested money is mostly directed to research & development, but some are used for acquisitions of AI companies.[38] The increased Chinese investments are

23. Barrington, *supra* note 18, at 81.
24. *Id.* at 82.
25. *Id*.
26. *Id*.
27. *Id*.
28. Zhu (Judy) Wang, *CFIUS Reforms in Context: China in the Crosshairs of CFIUS*, 30 AM. REV. INT'L ARB. 145, 146 (2019).
29. *Id*.
30. Barrington, *supra* note 18, at 83.
31. *Id*.
32. *Id*.
33. Zachary Arnold, *What Investment Trends Reveal About the Global AI Landscape*, BROOKINGS: TECHSTREAM (Sept. 29, 2020), https://www.brookings.edu/techstream/what-investment-trends-reveal-about-the-global-ai-landscape.
34. *Id*.
35. *Id*.
36. Justin Shields, *Smart Machines and Smarter Policy: Foreign Investment Regulation, National Security, and Technology Transfer in the Age of Artificial Intelligence*, 51 J. MARSHALL L. REV. 279, 282 (2018).
37. Wang, *supra* note 28, at 145.
38. Shields, *supra* note 36, at 282–83.

an indication of growing foreign interest in venture start-ups to gain new technology at its early development stage.[39]

The increase of foreign investments in AI is due the benefit it provides foreign countries like China because of its effects on those countries' tech sectors and more importantly the military.[40] AI would make surveillance much more efficient and reduce the human labor needed to do the same amount of work.[41] The United States believes that AI applications like these are important to the Chinese government because it increases their capability to conduct mass surveillance.[42] China has increased investments in domestic tech development, but it is looking toward foreign investments as a tool to gain access to the latest AI technology.[43]

While Chinese investments are increasing, they are still relatively minor players within the AI industry.[44] Chinese investments target various sectors of advanced manufacturing and American technology.[45] There is little evidence of Chinese investments targeting only defense-related AI.[46] However, despite the varied investments, the increase in foreign funding has raised flags for the United States. The U.S. fears that China may gain access to advanced technology that could be used in weapon systems and military technology.[47]

The United States is also concerned about the lack of market access in China to foreign investors.[48] China has been harsh on inbound foreign investment compared to the United States.[49] Oftentimes investments come with requirements such as having foreign investors as minority shareholders or having foreign investors give up their IP rights.[50] Moreover, the United States is also concerned about the interference of the Chinese government in private Chinese firms.[51] It is a blurry line that divides private companies and the government in China.[52] Chinese companies actively promote their connection to the Chinese Communist Party.[53] As part of their connection, these firms may gain access to U.S. technology by investing in and setting up companies within the United States, but because of their connection, the information housed within the U.S. may easily be accessed by the Chinese government.[54]

Additionally, there are a great number of government-owned companies, such as venture capital firms, that act on behalf of the Communist Party in

39. Barrington, *supra* note 18, at 101.
40. Shields, *supra* note 36, at 283.
41. *Id*.
42. *Id*. at 284.
43. *Id*. at 285–86.
44. Arnold, *supra* note 33.
45. Wang, *supra* note 28, at 152.
46. Arnold, *supra* note 33.
47. *See* Wang, *supra* note 28, at 154 (explaining that Chinese attempts to access the semiconductor sector has direct implications in all weapons systems and military technology).
48. *Id*. at 156.
49. *Id*.
50. *Id*.
51. Barrington, *supra* note 18, at 107.
52. Shields, *supra* note 36, at 290.
53. *Id*.
54. *Id*.

China.[55] They often advance the Party's goals and in response are financially backed by the government.[56] These government entities are subjected by law to assist the Chinese government in intelligence operations.[57] This close connection means that there is a possibility of these companies acting within the United States and giving the Chinese government access to developing technology.[58] Furthermore, there is limited access to records from these companies.[59] This leaves entities outside of China clueless about the extent to which information is transmitted to the Chinese government. To combat these concerns, the United States has turned to reevaluate its regulatory safeguards regarding foreign activity.[60]

B. Historical Approach to Foreign Investment & Development in the United States

Historically, the United States has taken an open economy-based approach to foreign investment and development within the United States.[61] Yet, recent national security concerns have led to a reevaluation of what foreign activity is acceptable within the country. The United States has used a variety of tools to halt foreign activity.[62] Translating this to the issue of TikTok, the United States may either ban the app or sell it to a U.S.-based company to prevent data from landing in the hands of the Chinese government.[63] In banning or forcing the sale of TikTok and other similar foreign applications, the President can look to IEEPA and CFIUS.[64]

The IEEPA is a statutory tool.[65] It provides broad power to the President to impose embargos and targeted sanctions (backed by the criminal law) on foreign entities in situations where U.S. interests are involved.[66] Under the IEEPA the President can freeze assets or ban financial activities of foreign organizations.[67] It allows the President to utilize economic power concerning major threats to U.S. national or economic security.[68] The process of acting under the IEEPA consists of a few steps.[69] The President first declares a national emergency and then assigns the threat to a specific executive agency to identify the denied

55. Wang, *supra* note 28, at 157 (noting that half of the Chinese economy is state-owned).
56. *Id*. at 158.
57. Barrington, *supra* note 18, at 107.
58. Wang, *supra* note 28, at 158.
59. *Id*.
60. *See id.* (noting that CFIUS now presumes all Chinese companies looking to invest in the U.S. are connected to the Chinese government and must convince the committee that they are not connected).
61. Barrington, *supra* note 18, at 81.
62. *See generally* Chesney, *supra* note 1 (discussing possible tools the U.S. can use against unsatisfactory foreign activity).
63. *Id*.
64. *Id*.
65. David R. Allman, *Scalpel or Sledgehammer? Blocking Predatory Foreign Investment with CFIUS or IEEPA*, 10 NAT'L SEC. L. BRIEF 267, 269 (2020).
66. Chesney, *supra* note 1.
67. *Id*.
68. Allman, *supra* note 65, at 271.
69. *Id*. at 284.

parties.[70] Lastly, based on the agency's designation, the Treasury Department's Office of Foreign Asset Control blocks the corresponding asset or transaction.[71] Under this act, everything rests on the President's ability to call a national emergency.[72]

While the IEEPA has a broad delegation, CFIUS requires a lower threshold for the U.S. to halt foreign activity like TikTok.[73] CFIUS is an interagency body that oversees the national security implications of foreign direct investment.[74] The original purpose of CFIUS was to persuade Congress not to enact restrictions on foreign investments in the 1970s.[75] CFIUS was formed by an executive order to review investments and give guidance on arrangements with foreign governments.[76] It was later backed by the signing of the International Investment Survey Act of 1976[77] which gave federal agencies the power to gather data for CFIUS to analyze. During this period CFIUS met a few times and operated with little action.[78] As concerns over foreign investments, especially from Japan, came up in the 1980s, Congress passed the Exon-Florio Amendment to the Defense Production Act.[79] This Act gave the President the power to block financial activities such as mergers and acquisitions if it affected national security.[80] At the same time, President Reagan delegated this statutory power to CFIUS giving them significant power in deciding what the President should do about foreign investments and acts.[81] Despite an increase in power, CFIUS still pursued few investigations and preferred to be generally accepting of foreign activity.[82] The Exon-Florio provision was later amended in 1992 by the "Byrd Amendment"[83] and extended CFIUS review on mergers, takeovers, and acquisitions if "(1) the acquirer is controlled by or acting on behalf of a foreign government; and (2) the acquisition results in control of a person engaged in interstate commerce in the United States that could affect the national security of the United States."[84] This amendment impacted foreign investors by allowing CFIUS to go back and review transactions it had already approved.[85]

70. *Id*.
71. *Id*. at 284–85.
72. *Id*. at 285
73. *See id.* at 328 (noting the CFIUS, unlike IEEPA, does not require a declaration of national emergency to block predatory investing).
74. James K. Jackson, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 1 (2020).
75. *Id*. at 4.
76. *Id*. at 5.
77. International Investment Survey Act of 1976, 22 U.S.C. §§ 3101–3108.
78. Wang, *supra* note 28, at 148.
79. *Id*.; Exon-Florio Amendment, 50 U.S.C. § 4565.
80. Jackson, *supra* note 74, at 7.
81. *Id*. at 8.
82. *Id*. at 6.
83. National Defense Authorization Act for Fiscal Year 1993, Pub. L. No. 102-484, § 837(a).
84. *Id*.
85. Jackson, *supra* note 74, at 10.

C. Present CFIUS

Concerns over China's increasing investments in the U.S. led Congress to modify CFIUS.[86] In 2018, Congress passed the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)[87] which expands the scope of transactions covered by CFIUS.[88] This provision provides CFIUS greater oversight over foreign investment within the United States.[89] It also allows consideration against investors from countries that are of "special concern."[90] FIRRMA covers foreign transactions such as mergers, acquisitions, or takeovers that could result in control by a foreign entity of a U.S. business.[91] FIRRMA also reviews a deal if it affects critical infrastructure, critical technology, or sensitive personal data, and if it does, then it is considered affecting national security.[92] FIRRMA was further embellished by a series of new regulations[93] in 2020 that asked CFIUS to investigate foreign investments that "maintains or collects sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security."[94] With FIRRMA, there has been an increase in regulation of foreign investment in the United States. CFIUS reviews have also increased due to growing concerns of cyber security.[95] The way the United States mitigates national security concerns under CFIUS review usually results in asking foreign companies to sell foreign assets, restricting certain technologies or access to locations, or submitting more information for additional inspections.[96]

D. TikTok & CFIUS

With the increased concern of Chinese involvement within the United States, TikTok is the latest application to be accused of as a Chinese tool for surveillance. TikTok has denied this claim. The application has tried to combat these rumors by stressing upon the American personnel within the company, including an American CEO, and denying that it has provided China with user data.[97] The app also argued that it has made public its content moderation policies to show transparency in the company's actions.[98] TikTok also considered the possibility of a sale to a U.S. based company to further show its

86. *Id.* at 11.
87. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No.115-232 (2018).
88. Jackson, *supra* note 74, at 1–2
89. *Id*.
90. *Id*. at 12.
91. *Id*. at 24.
92. *Id*.
93. 31 C.F.R. § 800.241 (2020).
94. Jackson, *supra* note 74, at 24.
95. Barrington, *supra* note 18, at 100–01.
96. Shields, *supra* note 36, at 292–93.
97. Zak Doffman, *Is TikTok Seriously Dangerous—Do You Need To Delete It?*, FORBES (July 11, 2020, 5:07 PM), https://www.forbes.com/sites/zakdoffman/2020/07/11/tiktok-seriously-dangerous-warning-delete-app-trump-ban/?sh=525d42b32b0e.
98. *Statement on the Administration's Executive Order*, TIKTOK (Aug. 7, 2020), https://newsroom.tiktok.com/en-us/tiktok-responds.

lack of connection to the Chinese government.[99] The app has made clear that the actions of the United States government against TikTok could undermine economic success within the U.S. and that the company is willing to sue the executive order forced against them.[100] Still the United States has not accepted any of the statements TikTok has made regarding this situation.

When TikTok (then called Music.ly) was bought by ByteDance, the app was considered a U.S. business that could be reviewed under CFIUS.[101] But CFIUS did not review the deal because national security was not a concern at the time of the purchase.[102] When TikTok grew in popularity, CFIUS, under its retroactive review power, began to analyze the transaction in November 2019.[103] At the end of the review, CFIUS ordered a divestment of TikTok, an order that remains in play today.[104] However, CFIUS did not set a deadline for when ByteDance must divest TikTok and stated it will not set a deadline after repeatedly granting extensions.[105]

In August of 2020, the government issued sanctions against ByteDance in an attempt to ban the application under the IEEPA's national emergency powers.[106] The government argued that TikTok threatened U.S. security due to its data collection practices on behalf of China.[107] The government also argued that sanctions are applicable under executive order 13873 which declares a national emergency based upon the threat of technology that is under the control of foreign entities.[108] However, that executive order deals with transactions on or after May 2019, a time later than the ByteDance acquisition.[109]

Things took a turn for TikTok in 2021. As President Biden took office, he revoked President Trump's sanctions, but his order left open the possibility for stronger sanctions on applications with foreign origins.[110] Biden's executive order reaffirms the validity of executive order 13873 and its sanction process, leading to the possibility that other applications may face what TikTok faced under the Trump Administration.[111] Yet even if TikTok is not banned or sold, the question remains of how the United States will review foreign-owned applications with national security implications.

---

99. *Id*.
100. *Id*.
101. Chesney, *supra* note 1.
102. *Id*.
103. *Id*.
104. Robert Chesney, *TikTok, WeChat, and Biden's New Executive Order: What You Need to Know*, LAWFARE (June 9, 2021, 1:09 PM), https://www.lawfareblog.com/tiktok-wechat-and-bidens-new-executive-order-what-you-need-know.
105. Kim Lyons, *Trump Administration Appeals Yet Another TikTok Ruling*, THE VERGE (Dec. 28, 2020, 3:21 PM), https://www.theverge.com/2020/12/28/22203284/trump-administration-appeal-tiktok-china-bytedance.
106. *Id*.
107. *See id*. (claiming President Trump feared for U.S. security interests based on China-based apps).
108. *See* Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 15, 2019) (allowing sanctions on technology and services that hinder national security).
109. Chesney, *supra* note 1.
110. Protecting Americans' Sensitive Data from Foreign Adversaries, 86 Fed. Reg. 31423 (June 9, 2021).
111. *Id*.

III. THE FLAWS OF A POTENTIAL U.S. RESPONSE TO TIKTOK

A. Ramifications of a Ban or Sale

National security concerns are necessary to consider regarding foreign activity within the United States. Yet the U.S. government must balance other interests with security. Looking at TikTok, a ban or sale has consequences beyond just the application.[112] Either action by the United States can have ripple effects on foreign and domestic entities within and outside of the United States.[113] It also leaves a dangerous precedent for the United States.

American companies are one of the biggest stakeholders that could be impacted by a TikTok ban or sale. A ban on applications like TikTok in the United States would lead to distrust among companies for fear of being banned internationally.[114] In the case of TikTok, if the United States imposes restrictions on China, it could risk losing access to the Chinese market for U.S. companies.[115] After the news of a possible ban on TikTok and other Chinese apps, China created a list of foreign companies it viewed that went against Chinese interests.[116] Though that list did not name any specific companies, it did indicate that the entities on that list may be barred from investing in China.[117] It also suggested fines and barring of employees from working within those companies.[118] China's retaliation list is not a new phenomenon. Before TikTok, the list was deliberated when the United States accused Huawei, a Chinese company, of stealing trade secrets and spying on behalf of China.[119] Furthermore, China has already blocked foreign internet services like Facebook and Google from operating within the country.[120] These acts demonstrate what China can do and what implications lie for American companies in China. For instance, Apple—which produces most of its products within China—could be penalized or fined by the Chinese government.[121] Other companies that could be affected are Amazon Web, which has joint cloud services within China, and Microsoft, which has a major market, research & development, and supply chains within the country.[122]

---

112. Keman Huang & Stuart Madnick, *The TikTok Ban Should Worry Every Company*, HARV. BUS. REV. (Aug. 28, 2020), https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company ("The proposed ban reinforces a growing belief that America is no longer the leading guarantor of global business, but rather a potential threat to it—a notion that is profoundly reshaping the world economy and threatening American businesses.").

113. Nachreiner, *supra* note 19.

114. Huang & Madnick, *supra* note 112.

115. Shields, *supra* note 36, at 304.

116. Keith Bradsher & Raymond Zhong, *After Trump's TikTok Ban, China Readies Blacklist of Foreign Companies*, N.Y. TIMES (Sept. 19, 2020), https://www.nytimes.com/2020/09/19/technology/china-tiktok-wechat-blacklist.html.

117. *Id*.

118. *Id*.

119. *Id*.

120. *Id*.

121. *Id*.

122. Nina Palmer, *Beijing's Retaliation on TikTok Could Hurt U.S. Firms*, FOREIGN POL'Y (Aug. 4, 2020, 12:21 PM), https://foreignpolicy.com/2020/08/04/china-retaliation-tiktok-could-hurt-american-firms-cisco.

China's possible retaliation also extends to if TikTok is sold to a U.S. buyer.[123] China views the ban or forced sale of TikTok as bullying and discrimination on the part of the United States.[124] However, it is necessary to note that American social media applications like YouTube, Gmail, and Snapchat are not allowed in China.[125] But retaliation by China could include continued discrimination against other U.S. applications.[126] China has accepted previous interference with forced sales of applications with Chinese origins. Grindr, a gay dating app with Chinese origins, was reversely purchased by a U.S. company.[127] However, TikTok is different. Part of China's ire comes from the popularity of TikTok.[128] TikTok is the first Chinese application with a significant market share in the United States.[129] Actions against TikTok could broadcast a broader message against China.

On the domestic front, the ban or sale could stall economic growth within the United States. For one, it would impact foreign investment in American technology.[130] Chinese investments are an important resource in tech sectors, specifically Silicon Valley.[131] One such company is China's Tencent, which owns WeChat (a Chinese messenger service) and is a strong investor in U.S.-based Reddit.[132] Additionally, previous precedent has shown the consequences of failed investments on U.S.-based companies.[133] In 2018, the United States rejected Qualcomm's merger with Broadcom, whose parent company, Avago, was based in Singapore.[134] This merger would have been the largest merger to date in the United States.[135] But just days before the merger, CFIUS met and recommended President Trump reject the deal.[136] Part of the rejection came from the fact that semiconductors, made by Qualcomm, can be used in tech equipment or, more specifically, radar equipment.[137] The government feared the radar equipment would be used for military purposes and prevented the deal from going through.[138] While there were no immediate consequences, the U.S. government's actions have created a possible hesitation for foreign companies to invest within the United States.[139] Along with a decline in investments,

123. Kenneth Rapoza, *China Promises To Retaliate If TikTok Forced To Sell*, FORBES (Aug. 7, 2020, 10:08 AM), https://www.forbes.com/sites/kenrapoza/2020/08/07/china-promises-to-retaliate-if-tiktok-forced-to-sell/?sh=666fbf946e1e.

124. *Id*.

125. *Id*.

126. Palmer, *supra* note 122.

127. *Id*.

128. *See id.* ("[T]his would mark the first time the U.S. government forced a Chinese-developed product with significant market share out of the U.S. market.").

129. *Id*.

130. Shields, *supra* note 36, at 298.

131. *Id*.

132. Matsakis, *supra* note 17.

133. Huang & Madnick, *supra* note 112.

134. Barrington, *supra* note 18, at 77.

135. *Id*.

136. *Id*. at 78–79.

137. *Id*. at 83.

138. *Id*.

139. Prachi Juneja, *The Aftermath of the Qualcomm Deal*, MGMT. STUDY GUIDE, https://www.managementstudyguide.com/aftermath-of-the-qualcomm-deal.htm (last visited Sept. 21, 2021).

another consequence is the redirection of foreign investment to countries with fewer restrictions.[140] The mere mention of a CFIUS investigation regarding a company can hurt the business's ability to complete a deal or gain investments.[141]

A ban or sale can have broader implications on competitive advantages within tech sectors.[142] There would be a reduction in U.S. companies having a competitive advantage over their competitors.[143] Though it would not be immediately seen, the gradual decrease in the presence of foreign companies and their technological advances could become an obstacle in U.S. research and development.[144] It reduces the spillover knowledge from foreign companies operating in the United States.[145] This also extends to Chinese talents who could make progressive steps in different tech sectors and create new developments within that field.[146] The U.S. government could stifle the growth of emerging technology and ideas.[147] It would hurt these fledgling companies from gaining investments to survive.[148] Also, with the increased and tightened regulations of CFIUS, companies must go through a rigorous regulatory process early in its development causing it to utilize a lot of its resources.[149]

As CFIUS became increasingly regulatory, there has been an upward trend towards prohibiting transactions rather than mitigating national security risks.[150] In TikTok's case, the company has implemented several changes to mitigate security risks.[151] The company has started storing data in the United States and backing it up in Singaporean servers.[152] It has also installed an American CEO and operations team while withdrawing from Hong Kong and setting up its global HQ somewhere else.[153] Furthermore, it even prevented parent company ByteDance from accessing user data from TikTok.[154] Yet the U.S. still pushed for the company to sell itself off, indicating that their actions have not calmed the government's concerns.[155]

The ban on applications such as TikTok does not prevent the risk of data collection from foreign governments.[156] The United States is at risk from Chinese data collection by other means as seen with the breaches at Anthem

140. Shields, *supra* note 36, at 299.
141. *Id*. at 294.
142. *Id*. at 298.
143. *Id*.
144. *Id*.
145. *Id*.
146. *Id*.
147. Wang, *supra* note 28, at 177.
148. *Id*.
149. *Id*.
150. Shields, *supra* note 36, at 296.
151. Huang & Madnick, *supra* note 112.
152. *Id*.
153. *Id*.
154. *Id*.
155. Wong, *supra* note 7.
156. Graham Webster, *App Bans Won't Make US Security Risks Disappear*, MIT TECH. REV. (Sept. 21, 2020), https://www.technologyreview.com/2020/09/21/1008620/wechat-tiktok-ban-china-us-security-policy-opinion.

Health Insurance and Equifax.[157] With the weaknesses in U.S. systems, if entire tech sectors are penalized, it could lead to negative effects on innovation within the United States.[158]

In the realm of domestic policy, a TikTok ban can be detrimental to the U.S. government's data collection. The United States is among the many countries that want to gain access to user data in applications.[159] However, in fear of China, Silicon Valley firms will hesitate to work with the U.S. government on a policy basis in fear of losing out on the Chinese market.[160] Additionally, if development is halted within the United States, the country will not be able to adapt to new technologies for governmental purposes.[161] This could lead to distance between the U.S. government and developing technology, which could hinder regulation of such technology by the government and result in weaknesses within the country's security.[162]

Under foreign policy, a hard approach to foreign apps could impact trade ties with other countries.[163] For example, China is a major importer of agricultural goods and lumber.[164] If China decides to reduce imports, it could impact the economies of agricultural states who are the key producers of these resources.[165] China could also retaliate with forced sales of Chinese assets by U.S. entities.[166] It could also lead to foreign companies searching for alternative suppliers for U.S. components of their products in different countries to avoid regulatory uncertainty.[167]

One other implication is the possibility of splinternets. The United States is at the forefront of the fight for an open democracy.[168] However, with countries putting up barriers, it leads to a phenomenon called splintering.[169] Splintering is the carve-up of the internet into different regional areas,[170] essentially creating a digital border wall that separates the internet of one country from everyone else.[171] One way this occurs is through the management of a filter to allow certain data into the country.[172] This includes information such as keywords and IP addresses.[173] This is China's approach, but countries like Russia are taking a

157. *Id*.
158. Allman, *supra* note 65, at 339.
159. Huang & Madnick, *supra* note 114.
160. Shields, *supra* note 36, at 304.
161. Wang, *supra* note 28, at 177.
162. Shields, *supra* note 36, at 300.
163. Rapoza, *supra* note 123.
164. *Id*.
165. *Id*.
166. Palmer, *supra* note 122.
167. Huang & Madnick, *supra* note 112.
168. VOX, *The Problem With Banning TikTok*, YOUTUBE (Aug. 29, 2020), https://www.youtube.com/watch?v=BAsXGN2OX0c.
169. Editorial Board, *TikTok And The Splintering Of The Global Internet*, FIN. TIMES (Aug. 3, 2020), https://www.ft.com/content/6a1b9b4d-ddbc-4b62-9101-221510fb7b45.
170. *Id*.
171. Sally Adee, *The Global Internet Is Disintegrating. What Comes Next?*, BBC: FUTURE (May 14, 2019), https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.
172. *Id*.
173. *Id*.

slightly different stance.[174] They aim to keep internet traffic within their geographical borders, not to the outside world.[175] Besides the obvious free speech violations, splintering has bigger impacts on countries. For one, it can slow innovation.[176] Lack of access to internet resources stifles innovation and growth.[177] The Internet pushes for collaboration. A ban on TikTok would create a splinternet, keeping the United States from the connected world within the application. Additionally, if the U.S. takes this path, it sends a message to other countries to emulate this action.[178] Research supports that many countries are moving towards a more closed internet.[179] Countries take this path for national security reasons.[180] This is a valid concern, but the consequences of a splinternet are vast and global. If the United States moves in this direction, it would be a country that loses its foothold as a defender of an open internet.[181]

B. Bypassing of a U.S. Response

Banning or selling applications like TikTok can have widespread ramifications. However, the current methods to bypass these bans or force sales are ineffective in solving the consequences that can occur. Additionally, there is no worthwhile way for a company to fight against a U.S. response, especially in the situation of TikTok. The methods that do exist leave a wide gap for foreign entities to exploit for national security purposes.[182] In TikTok's case, there is no viable option to stop a ban or sale of the app if it were to go through and at the same time balance security concerns by the government.[183]

Before FIRRMA, TikTok would have been unable to litigate a CFIUS order if it did not rule in their favor.[184] CFIUS orders were not subject to regular judicial review.[185] Even if the company were to challenge the executive order banning TikTok, challenging an executive order by the President becomes difficult due to the authority given to the President in matters of foreign affairs and national security.[186] The Exon-Florio Amendment stated that courts did not have the authority to review presidential decisions to suspend or block a deal.[187]

However, the D.C. Circuit has allowed for constitutional claims to still come forward concerning CFIUS orders.[188] In *Ralls v. CFIUS*, Ralls Corporation, a Chinese company, sued CFIUS to challenge CFIUS's decision to

174. *Id*.
175. *Id*.
176. *TikTok And The Splintering Of The Global Internet*, *supra* note 169.
177. *TikTok And The Splintering Of The Global Internet*, *supra* note 169.
178. Adee, *supra* note 171.
179. *Id*.
180. *Id*.
181. *The Problem With Banning TikTok*, *supra* note 168.
182. Chesney, *supra* note 1.
183. *Id*.
184. *Id*.
185. *Id*.
186. Ari K. Bental, *Judge, Jury, And Executioner: Why Private Parties Have Standing to Challenge an Executive Order that Prohibits ICTS Transactions with Foreign Adversaries*, 69 AM. U.L. REV. 1883, 1922 (2020).
187. *Id*. at 1910.
188. Chesney, *supra* note 1.

block a wind-farm construction plan.[189] On appeal, the appellate court held that while Ralls could not challenge the President's conclusion regarding the transaction in question because it was a question of national security, it could challenge based on the company's Fifth Amendment due process rights being violated.[190] The government could deprive a party of its due process rights when it does not give adequate notice of its action, access to unclassified evidence, or the opportunity to rebut that evidence.[191] In *Ralls*, the government did not provide Ralls with the information the President used to determine why the plan should be vetoed.[192]

But *Ralls* is no longer an obstacle given that FIRRMA has created a formal avenue for judicial review of CFIUS orders by requiring the filing of challenges to the D.C. Circuit Court.[193] In another jurisdiction, a district court judge in Washington issued a preliminary injunction to prevent the Commerce Department from preventing the removal of TikTok from application stores in the United States.[194] This court eventually issued an order that prevented the Commerce Department from preventing new downloads of the application.[195] The Department of Justice has filed an appeal to the D.C. Circuit Court to decide whether national security concerns are enough to justify a ban on TikTok.[196] A couple of months later, another federal judge in Pennsylvania blocked the Commerce Department from barring TikTok from operating in the United States.[197] This means that the Commerce Department cannot prevent TikTok from data hosting, content delivery, or other such actions from happening in the United States.[198] In response to its actions, the court stated that the government's national security concerns are "hypothetical."[199] On the other hand, TikTok has filed an appeal to the U.S. Court of Appeals to review the actions of CFIUS as it has not been responsive about when its parent company ByteDance must sell off its U.S. assets due to national security concerns.[200] Currently, the Department of Justice has asked the cases to be dismissed for mootness due to the revocation of President Trump's executive order.[201] However, despite this outcome, the question remains if the broad discretion given to the executive branch on foreign

189. Ralls Corp. v. CFIUS, 758 F.3d 296, 301–02, 304 (D.C. Cir. 2014).
190. *Id*. at 319–20.
191. *Id*.
192. *Id*.
193. Bental, *supra* note 186, at 1911.
194. David Shepardson, *U.S. Will 'Vigorously Defend' Tiktok Executive Order Despite Ruling*, REUTERS (Nov. 1, 2020, 2:54 PM), https://www.reuters.com/article/us-usa-tiktok-ban/u-s-will-vigorously-defend-tiktok-executive-order-despite-ruling-idUSKBN27H1R7.
195. Lyons, *supra* note 105.
196. *Id*.
197. Shepardson, *supra* note 194.
198. *Id*.
199. *Id*.
200. Sam Byford, *TikTok Says the Trump Administration Has Forgotten about Trying to Ban it, Would Like to Know What's Up*, THE VERGE (Nov. 10, 2020, 9:09 PM), https://www.theverge.com/2020/11/10/21559677/ tiktok-cfius-court-petition-ban-deadline.
201. David Shepardson, *Biden Administration asks Courts to Dismiss Government Appeals of TikTok Ruling*, REUTERS (July 12, 2021, 6:41 PM), https://www.reuters.com/business/retail-consumer/us-asks-court-dismiss-government-appeal-tiktok-ruling-2021-07-12.

matters would allow the ban or sale on applications like TikTok. Furthermore, litigation is a tedious and ineffective method to bypass CFIUS decisions.

The other method to bypass CFIUS is through the gaps in its review process. One of CFIUS's gaps pertains to startups.[202] CFIUS, while expanding its coverage on a range of issues, fails to take into consideration investments in venture startups, where many national security concerns originate.[203] FIRRMA specifically fails to address critical issues and fails to serve CFIUS in addressing national security concerns regarding cyberwarfare.[204] Additionally, ambiguous terms play a negative role on companies. For one, FIRRMA lowers the benchmark of what triggers a review.[205] FIRRMA covers any investment, direct or indirect, that deals with giving a foreign person access to resources that can influence a company's involvement in "sensitive personal data; critical technologies; or critical infrastructure."[206] This broad delegation is unclear about what constitutes "influence" over a company.[207] This ambiguity carries over to other provisions such as the undefined term "sensitive personal data."[208] The vagueness in CFIUS has the potential to harm economic prosperity because it creates uncertainty for companies that deal with sensitive personal data.[209] An unclear process hinders the ability of companies, like TikTok, to follow CFIUS and confidently invest or operate within the United States.[210] These gaps in CFIUS may be exploited by foreign companies and hinder the U.S.'s ability to balance between national security concerns and emerging foreign activity within the country.[211]

There is also the possibility of simply avoiding CFIUS.[212] If a foreign entity creates a subsidiary within the United States, it may, in the short-term, conduct research and development with American innovators and avoid CFIUS until a later time.[213] If a startup investment is not associated with an existing U.S. entity, then CFIUS does not review it, and as a result, companies can bypass CFIUS.[214] Foreign entities need to just invest early on by employing creators of new technology.[215] This action inhibits the ability for CFIUS to overlook legitimate threats of national security that could arise. However, while possible for other companies, TikTok would be unable to avoid CFIUS due to it being a retroactive review by the Committee.[216]

Besides simply bypassing or avoiding CFIUS, the review process itself is ineffective to solve security concerns and balance foreign activity. Several

202. Barrington, *supra* note 18, at 120.
203. *Id*. at 103.
204. *Id*. at 80.
205. *Id*. at 106.
206. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No.115-232 (2018).
207. Barrington, *supra* note 18, at 106.
208. *Id*. at 110.
209. *Id*.
210. *Id*.
211. *Id*. at 121.
212. *Id*. at 120.
213. *Id*.
214. *Id*. at 121.
215. *Id*.
216. Chesney, *supra* note 1.

CFIUS reviews show the inconsistency of CFIUS towards foreign activity.[217] In April 2017, Ant Financial, a Chinese company, wanted to buy MoneyGram to expand its online payment system.[218] However, the deal was blocked by CFIUS due to concerns over the possibility of Ant Financial giving China access to large records of financial information and using that information as leverage against U.S. officials.[219] The deal even considered storage of personal data within the U.S., but even with these concessions, the deal was denied.[220] On the flip side, China Oceanwide, a financial holding group, made a deal with Genworth Financial, a long-term-care insurance company based in Virginia.[221] This deal would have allowed Oceanwide to access the personal data of U.S. insurance holders.[222] However, this deal passed a long review by CFIUS after the companies agreed to use a U.S.-based third-party service provider to manage U.S. policyholders.[223] Both deals dealt with data of U.S. citizens, but it is unclear what sets them apart. It may have been the keeping of U.S. data onshore and away from China, but the United States was not willing to concede even after Ant Financial was willing to store their data within the United States.[224] This inconsistency has carried over to TikTok. TikTok has argued that it would store data outside of China and would not grant China access to the data.[225] But CFIUS has not approved of this argument.[226] These irregular actions create uncertainty in the mitigation tactics used by companies to battle against increased regulation regarding foreign applications in the United States.[227] It also hinders the confidence of companies to invest within the United States.[228]

If a ban or sale were pushed under the IEEPA, challenges to those decisions would be unsuccessful. The broad designation of power to the President regarding foreign affairs makes it difficult to combat the banning of apps like TikTok.[229] Yet the need for an emergency is vital for the IEEPA to go into action. Additionally, the court has held that in blocking companies under the IEEPA, it is necessary to have a valid reason for the investigation and the need for disclosure to companies on why their assets were being blocked.[230] Best seen in the case of *Dames & Moore*, the Supreme Court held that the President has substantial power in foreign affairs.[231] Additionally, if the United States has

217. Alan Rappeport, *U.S. Outlines Plans to Scrutinize Chinese and Other Foreign Investment*, N.Y. TIMES (Sept. 17, 2019), https://www.nytimes.com/2019/09/17/us/politics/china-foreign-investment-cfius.html.

218. Wang, *supra* note 28, at 161.

219. *Id*.

220. *Id*. at 162.

221. *Id*.

222. *Id*.

223. *Id*.

224. *Id*.

225. *Statement on Tiktok's Content Moderation and Data Security Practices*, TIKTOK (Oct. 24, 2019), https://newsroom.tiktok.com/en-us/statement-on-tiktoks-content-moderation-and-data-security-practices.

226. *See* Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297 (Aug. 14, 2020) (ordering ByteDance to divest TikTok after CFIUS review).

227. Farah Lalani, *Banning Apps Like TikTok is a Slippery Slope. Here's Why*, WORLD ECON. F. (Nov. 25, 2020), https://www.weforum.org/agenda/2020/11/banning-apps-like-tiktok-slippery-slope.

228. *Id*.

229. Allman, *supra* note 65, at 298.

230. *Id*. at 306.

231. Dames & Moore v. Regan, 453 U.S. 654, 654 (1981).

control of foreign assets, it is used as bargaining power.[232] There are only a few cases where federal courts limited the power of IEEPA for due process claims, but they still deferred strong power to the President in the realm of national security.[233] Even so, the Supreme Court has given deference to the government on foreign matters.[234] Based on this, a ban or sale on apps like TikTok may go through under IEEPA.[235]

C. Learning from the EU Approach

Compared to the United States, Europe's evaluation of foreign actions is separated based on issues. In Europe, no one body manages the actions of foreign companies within its boundaries.[236] Regarding FDI, until recently, there has not been a CFIUS level regulation. In 2019, the European Union set up an EU-level framework (the "Regulation") to deal with foreign direct investment in the EU.[237] The Regulation is the first EU-level mechanism that screens "foreign investments likely to affect the security and public order of the Union and its Member States."[238] Previously the EU stated it would independently screen out FDI.[239] The EU's change in policy was developed based on the possibility that a company in one member state could affect another member state.[240] The EU's CFIUS-like counterpart oversees acquisitions of European companies by foreign organizations.[241] One of the factors the European Union Commission (the "Commission") looks at is "the effects on critical infrastructure, technologies, and inputs."[242] The Commission also looks to see if sensitive personal data could be accessed or controlled by those foreign companies.[243] Like CFIUS, the Commission considers if a foreign company is controlled by "the government of a third country or is pursuing state-led outward projects or programs."[244] The Regulation does not consider a foreign investor's origin and it makes clear that it carries a non-discrimination principle.[245] News surrounding the Regulation

232. *Id*. at 673–74.

233. *See* Al-Haramain Islamic Foundation, Inc. v. U.S. Department of Treasury, 686 F.3d 965 (9th Cir. 2012) (limiting the scope of IEEPA); United States v. Arch Trading Co., 987 F.2d 1087, 1087 (4th Cir. 1993) (holding that the IEEPA cannot create crimes); KindHearts for Charitable Humanitarian Development, Inc. v. Geithner, 710 F. Supp. 2d 637 (N.D. Ohio 2010) (limiting the IEEPA).

234. Thomas Matthew Mashburn, *Regan v. Wald, The Supreme Court Defers to Presidential Authority in Matters of Foreign Policy by Upholding Travel Restrictions to Cuba*, 15 GA. J. INT'L & COMP. L. 83, 83 (1985).

235. Chesney, *supra* note 1.

236. Commission Regulation 2019/452, Establishing a Framework for The Screening of Foreign Direct Investments into the Union, 2019 O.J. (L79) 1.

237. *Id*.

238. *Coronavirus: Commission Issues Guidelines to Protect Critical European Assets and Technology in Current Crisis*, EUR. COMM'N (Mar. 25, 2020), https://trade.ec.europa.eu/doclib/press/index.cfm?id=2124.

239. European Commission Memorandum, Frequently Asked Questions on Regulation (EU) 2019/452 Establishing a Framework for the Screening of Foreign Direct Investments into the Union 3 (June 22, 2021) [hereinafter Commission Memo].

240. *Id*.

241. *Id*.

242. *Id*. at 4.

243. *Id*.

244. *Id*.

245. Commission Regulation 2019/452, Establishing a Framework for the Screening of Foreign Direct Investments into the Union, 2019 O.J. (L79) 1.

does not name a country to which this screening will apply, a difference to CFIUS whose information points to the growing national security concern of China.[246] The EU still seeks to be open to FDI within the country.[247] However, the EU screening is not the same as each member state's screening.[248] Rather it shares information on which FDI could affect surrounding member states.[249]

Through this Regulation, the Commission recommends a course of action to the EU member states involved with the FDI. However, the responsibility falls on the member state for its national security.[250] They are ultimately responsible for the final decision as to if an investment will occur in that member State.[251] Foreign investors have an opportunity of recourse against screening decisions.[252] This cooperation mechanism only lasts fifteen months after the investment is completed.[253] This differs from CFIUS, as the EU Commission cannot block, review, or impose.[254] Instead, the EU Commission leaves that in the hands of the individual member states.[255] It also has in place a judicial review function for decisions.[256]

In cases with the EU and China, the EU has taken a different approach than the United States. The EU is China's biggest trading partner.[257] Conversely, European companies have become prime investors in China.[258] However, China's increased investment in European assets triggered the EU.[259] In addressing this concern, the EU did not want to take a CFIUS approach like the United States.[260] The Regulation was the EU's solution to balance open investment and the security concern of China's increasing presence within the EU.[261]

Another approach the EU took was to reevaluate data privacy within its borders. The European Union passed the General Data Protection Regulation (GDPR) that compiled all laws on data privacy.[262] The goal of the GDPR was to have companies place their focus "by design and by default" on data

246. *EU Foreign Investment Screening Mechanism Becomes Fully Operational*, EUR. COMM'N (Oct. 9, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867; CONGRESSIONAL RESEARCH SERVICES, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 11 (2020).

247. Commission Memo, *supra* note 239, at 4.

248. *Id*. at 5.

249. *Id*.

250. Commission Regulation 2019/452, Establishing a Framework for the Screening of Foreign Direct Investments into the Union, art. 3, 2019 O.J. (L79) 1.

251. Commission Memo, *supra* note 239, at 12.

252. Commission Regulation 2019/452, Establishing a Framework for the Screening of Foreign Direct Investments into the Union, art. 3, 2019 O.J. (L79) 7.

253. Commission Memo, *supra* note 239, at 14.

254. Michael S. Casey et al., *New EU Foreign Direct Investment Regulations Take Effect*, KIRKLAND & ELLIS (Oct. 29, 2020), https://www.kirkland.com/publications/kirkland-alert/2020/10/eu-fdi-regulation.

255. *Id*.

256. Yaniss Aiche, *The Traps of a CFIUS Like EU FDI Screening Mechanism*, NAT'L. L. REV. (Nov. 29, 2018), https://www.natlawreview.com/article/traps-cfius-eu-fdi-screening-mechanism.

257. *Id*.

258. *Id*.

259. *Id*.

260. *Id*.

261. *Id*.

262. Barrington, *supra* note 18, at 109.

protection.[263] The EU approach is to focus on how businesses operate within the country rather than prevent its entry.[264] It created laws on data control and security that forced foreign companies, such as Facebook, to follow in order to operate within its borders.[265] Violation of these laws could lead to repercussions or fines for the company.[266]

In Europe, ByteDance is facing scrutiny under the GDPR, not its FDI Regulation.[267] These inquiries, as compared to the U.S. probe, would be less politically based and more likely to address the problems concerning national security.[268] TikTok, under the GDPR, has a higher level of responsibility given that it deals with data related to children, a group that gets more protection under the GDPR.[269] Individual countries in Europe will continue investigating TikTok till it establishes a main data processing center in the EU.[270] Once that is established, the review moves to the country in which the data processing center is located.[271] Without this data processing center, TikTok would be under question by member states all over the EU.[272] Many of these probes towards TikTok deal with data privacy.[273] The probes look to see how user data is processed, access to data, transfer of data outside the UK, and the protection of minor's data.[274] If TikTok follows EU law, it will not be banned from Europe.[275] Though one flaw under this process is that it leaves open the question of who regulates the application until the creation of a data processing center within the EU.[276]

IV. RECOMMENDATIONS

To balance national security concerns and prevent ramifications of a ban or sale, this Note recommends a clear, rigorous, and nondiscriminatory approach to foreign activity under CFIUS and a strengthening of statutory protections for data security. A rigorous but non-discriminatory approach can ease national security concerns and allow foreign applications to operate within the United States. As the CFIUS approach is modified, statutory protections would allow

263. Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/?cn-reloaded=1 (last visited Sept. 12, 2020).

264. Corey Nachreiner, *In Defense of TikTok and Foreign-Based Apps, Part Two*, FORBES (Aug. 4, 2020) https://www.forbes.com/sites/forbestechcouncil/2020/08/04/in-defense-of-tiktok-and-foreign-based-apps-part-two.

265. *Id*.

266. *Id*.

267. Saqib Shah, *Tiktok Privacy Probes in Europe Raise Stakes for Local Data Handling*, S&P GLOB. MKT. INTELLIGENCE (Oct. 1, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/tiktok-privacy-probes-in-europe-raise-stakes-for-local-data-handling-60562927.

268. *Id*.

269. *Id*.

270. *Id*.

271. *Id*.

272. *Id*.

273. *Id*.

274. *Id*.

275. *Id*.

276. *Id*.

data security concerns to be handled more clearly outside of CFIUS's jurisdiction.[277]

A clear review of foreign companies is better than a forced sale or ban of foreign investments and operations.[278] CFIUS should take a case-by-case analysis in understanding the application rather than running a simple review and placing emphasis on an application's country of origin.[279] However, CFIUS would have to make sure that it does not express a discriminatory approach by only reviewing applications with a certain origin. Rigorous regulation is a necessity for the United States to maintain national security concerns. It is part of what countries do. They oversee security concerns when foreign activity occurs within its borders.[280] The United States can be aware that China may play a bigger role due to the power it holds. But that should not be a vital factor in the review of foreign activity from that country.

In creating a rigorous review system, CFIUS should clarify its process. This includes outlining specific examples of technologies that would trigger national security interests and keep companies with that technology on notice.[281] This information can be used to evaluate recent technology and specific applications that come into the country. In TikTok's case, CFIUS should ask TikTok to open its software to understand how the application works.[282] CFIUS also mentions the regulation of actions that deal with "sensitive personal data."[283] Yet, it is unclear what this phrase means and how companies would go about solving it. This inconsistency, as mentioned earlier in this Note, has no clear process to solve this issue.[284] CFIUS should list out clear guidelines to prevent "sensitive personal data" from being accessed by foreign entities. In the case of TikTok, it could force the company to formulate regulations that prevent access to sensitive data to those outside the United States.[285] In addition, there should be a clear threshold of when companies have met the necessary standards to operate within the United States. Unlike the situation with Ant Financial, CFIUS should clarify what requirements would enable foreign companies the right to operate within the United States. The push should be towards transparency in the CFIUS review process rather than an incomprehensible ban. The fear of TikTok comes from the lack of transparency on who can access TikTok's data.[286]

277. Bergman et al., *supra* note 6.

278. Nachreiner, *supra* note 19; *see also* Protecting Americans' Sensitive Data from Foreign Adversaries, 86 Fed. Reg. 31423, 31423 (June 9, 2021) (calling for the federal government to create a rigorous process in determining national security risks).

279. Shields, *supra* note 36, at 305.

280. JOHN M. BEAHN ET AL., SHEARMAN & STERLING, CFIUS AND BEYOND: NAVIGATING THE COMPLICATED UNIVERSE OF REGULATORY AND OTHER CONSTRAINTS RELATED TO US NATIONAL SECURITY 2 (2020).

281. Bental, *supra* note 186, at 1937.

282. Kevin Roose, *Don't Ban TikTok. Make an Example of It*, N.Y. TIMES (July 26, 2020), https://www.nytimes.com/2020/07/26/technology/tiktok-china-ban-model.html.

283. Barrington, *supra* note 18, at 110.

284. Rappeport, *supra* note 217.

285. Roose, *supra* note 282.

286. *Id*.

A rigorous and clear review should also focus on the security of the data present in apps like TikTok. CFIUS should list out steps or recommendations that force foreign applications to manage these risks. In TikTok's case, there have been cybersecurity flaws found within the app.[287] Weaknesses in the app have left openings for hackers to exist.[288] CFIUS should force TikTok to solve these kinds of security weaknesses and in turn manage the security concern of data security. As companies like TikTok grow, data concerns will always be present. Yet that should not hinder the growth of a company. As one expert puts it, the ability for a foreign company to have our data should not be the cutoff point.[289]

To supplement rigorous and clear CFIUS review, the United States should set up clear statutory protections for data. The government's main concern about TikTok is the data it has access to.[290] While CFIUS may put in place clear guidelines on data management for foreign companies, the United States should set up clear internal guidelines separate from CFIUS. Like the EU setting up the GDPR, the United States' statutory protections would relieve some of CFIUS's burden in managing data protection and security concerns. In the EU, the Commission is scrutinizing TikTok under the GDPR rather than FDI screening.[291] While their FDI screening is aware of the data concerns regarding foreign activity, it does not have to direct all its foreign concerns to one body for review.

There has been a push for the United States to develop a federal statutory standard to cover how data should be handled no matter if they originate from foreign or domestic entities.[292] Expanding a federal statute to domestic entities is beneficial in combatting foreign hacks on domestic companies.[293] It also allows for a clearer understanding for companies on how to manage data within the United States.[294]

Following the GDPR, many states have enacted their version of a privacy law.[295] Recently, California has implemented the most expansive data privacy regulation with the enactment of the California Consumer Privacy Act of 2018 (CCPA).[296] The CCPA allows Californians, among other rights, to know which information a business collects on them, the right to have certain information deleted that has been collected, and the right to prevent the sale of their

287. Bergman et al., *supra* note 6.
288. *Id*.
289. *Id*.
290. McMillan et al., *supra* note 8.
291. Shah, *supra* note 267.
292. Samm Sacks, *Banning Tiktok Is a Terrible Idea*, SUPCHINA (July 26, 2020), https://supchina.com/2020/07/16/banning-tiktok-is-a-terrible-idea.
293. *Id*.
294. *Id*.
295. Sedgwick Jeanite, *Data Protection Laws: Following GDPR Enactment, US States Take Action*, WHITE & WILLIAMS (Mar. 8, 2019), https://cyber.whiteandwilliams.com/2019/03/data-protection-laws-following-gdpr-enactment-us-states-take-action.
296. Maureen Mahoney, *California Has a Privacy Law, but Will Companies Comply?*, THE HILL (Feb. 11, 2020, 12:30 PM), https://thehill.com/opinion/cybersecurity/482478-california-has-a-privacy-law-but-will-companies-comply.

information.[297] As California has expanded its data privacy laws, the rest of the country has followed with each state enacting its own data privacy laws resulting in a fragmented approach to data privacy.[298]

However, a fragmented approach makes it difficult for foreign companies to manage the multiple regulations.[299] To allow for growth and development, the United States must put forward a federal approach. By creating a uniform policy, the United States can address national security regarding all the people that fall under the policy's jurisdiction. This also makes it easier to address national security concerns regarding foreign entities rather than having each state take its own approach to foreign companies.

V. CONCLUSION

The United States has been an open market that allows in ideas and, more importantly, activities from foreign investors and entrepreneurs. However, the increasingly global nature of the world has put national security concerns, especially in the realm of data privacy, at the forefront. This issue has come to head most recently with TikTok. As the app has increased in popularity, the United States has debated the ban or sale of the app due to concerns about its Chinese origins and data access.

While the current administration has not yet decided its approach to TikTok, the decision the U.S. government makes could have ramifications far beyond the application. Other methods of going around CFIUS decisions are ineffective and cumbersome for foreign companies wanting to operate within the United States. However, the example of the EU gives some guidance on how the U.S. should approach applications like TikTok. There needs to be a rigorous, clear, and nondiscriminatory review process within CFIUS supplemented by the strengthening of internal statutory protections. With these changes, the United States will be able to strike a balance between national security concerns and foreign activity growth. Yet, as it stands now, the fate of applications like TikTok hangs in the air waiting for the United States to decide on its future.

297. CAL. CIV. CODE § 1798.100 (2020).

298. *See generally* Florian Schaub, *Fragmented U.S. Privacy Rules Leave Large Data Loopholes for Facebook and Others*, SCIENTIFIC AM. (Apr. 10, 2018), https://www.scientificamerican.com/article/fragmented-u-s-privacy-rules-leave-large-data-loopholes-for-facebook-and-others.

299. *Id*.