A BULL IN A CHINA SHOP: HOW CFIUS MADE TIKTOK A NATIONAL SECURITY PROBLEM

Adina Feder[†]

TABLE OF CONTENTS

I. INTRODUCTION

On August 6, 2020, the Trump Administration issued an executive order effectively banning the usage of the popular social media application, TikTok, owned by Chinese company ByteDance Ltd., reasoning that it was a threat to national security.[1] President Trump claimed that, due to its mass data collection and foreign ownership, TikTok threatens to allow "the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[2] TikTok, a global video sharing app, is currently used by 100 million Americans.[3] It gathers substantive information about its users including:

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

---

† J.D., Benjamin N. Cardozo School of Law, 2022. I would like to thank Professor Wu for providing helpful advice, critiques, and comments throughout the development of this Note.

1 Exec. Order No. 13942, 85 Fed. Reg. 48,637 (Aug. 6, 2020). The President also separately ordered ByteDance to divest itself of TikTok's U.S. operations, including any interest it might have in U.S. user data. *See* Order of August 14, 2020, Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 19, 2020).

2 Exec. Order No. 13942, 85 Fed. Reg. at 48,637; *see also* Greg Roumeliotis, Yingzhi Yang, Echo Wang & Alexandra Alper, *Exclusive: U.S. Opens National Security Investigation into TikTok - Sources*, REUTERS (Nov. 1, 2019), https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL [https://perma.cc/NVV8-YHBD]; Nancy Marshall-Genzer, *What's CFIUS and What Does It Have to Do with TikTok?*, MARKETPLACE (Aug. 5, 2020), https://www.marketplace.org/2020/08/05/what-is-cfius-tiktok [https://perma.cc/S696-JKSU].

3 Marland v. Trump, No. CV 20-4597, 2020 WL 5749928, at *1, 2 (E.D. Pa. Sept. 26, 2020) ("In the United States, TikTok currently has more than 100 million active monthly users and 50 million active daily users.").

> challenges, sweepstakes, or contests such as gender, age, likeness, and preferences.[4]

TikTok is one of hundreds of foreign owned companies which contribute hundreds of billions of dollars annually to the U.S. economy. In fact, it has been said that "[w]here globalization is a defining trait of the modern era, foreign direct investment [("FDI")] is its lifeblood."[5] In enacting the statutory regime to regulate the enormous and ever-growing presence of FDI, Congress made many of the following findings.[6] According to a 2016 report written by the International Trade Administration for the Chamber of Commerce, approximately 8.5% of the labor force, or twelve million U.S. workers, have jobs from foreign investment.[7] The manufacturing sector alone contains 3,500,000 jobs from foreign investment, and in 2016, new FDI in manufacturing totaled $129,400,000,000.[8] The Bureau for Economic Analysis found that in 2015, foreign owned affiliates in the United States contributed $894,500,000,000 to the U.S. economy, exported about one quarter of the total exported goods, valued at $352,800,000,000, and spent $56,700,000,000 in research and development.[9] Further, since Congress made their findings, The Bureau of Economic Analysis compiled the data that between 2019 to 2020, foreign direct investment in the U.S. increased by $187.2 billion to a whopping $4.63 trillion, mainly in the manufacturing, finance, insurance and wholesale trade industries.[10]

The issue is that FDI has serious implications for national security "necessitating policies that balance economic interest with

---

4 TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 99 (D.D.C. 2020).

5 Christopher M. Fitzpatrick, *Where Ralls Went Wrong: CFIUS, the Courts, and the Balance of Liberty and Security*, 4 CORNELL L. REV. 1087, 1088 (2016); *see also* Andrew Burke, Holger Görg & Aoife Hanley, *The Impact of Foreign Direct Investment on New Firm Survival in the UK: Evidence for Static Versus Dynamic Industries*, 31 SMALL BUS. ECON. 395, 395 (2008) (noting that FDI is "likely . . . the most important aspect of globalisation in economic terms"); EDWARD M. GRAHAM & PAUL R. KRUGMAN, FOREIGN DIRECT INVESTMENT IN THE UNITED STATES 57–59 (3d ed. 1995) (recognizing three primary sources of economic gain: "comparative advantage" through trade enabled specialization, "increasing returns to scale," and "increased competition").

6 Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(a), 132 Stat. 2174.

7 *Id.* § 1702 (a)(1).

8 *Id.* § 1702(a)(1)–(2).

9 *Id.* § 1702(a)(3)(i)–(iii).

10 News Release, Bureau of Econ. Analysis, Direct Investment by Country and Industry, 2020 (July 22, 2021) (available at https://www.bea.gov/news/2021/direct-investment-country-and-industry-2020 [https://perma.cc/3JKL-22AK]).

precautionary measures."[11] For the 2017–2019 period, acquisitions by investors from China accounted for twenty percent (or 140 Committee on Foreign Investment notices), the largest proportion of notices filed.[12] Thus, as any good sovereign country would do and has done, America "has sought to temper its embrace of open markets with the protection of its national security interests."[13]

To effectuate such policies, all transactions or investments involving foreign entities in U.S. business or U.S. real estate interests are assessed by the Committee on Foreign Investment ("CFIUS" or "Committee"), an interagency body which reviews any mergers, acquisitions, and other transactions which can result in foreign ownership or control of a U.S. business, for potential national security concerns.[14] The determination is then passed along to the U.S. President, who has the authority to block transactions or acquisitions pursuant to the International Emergency Economic Powers Act ("IEEPA") and the National Emergencies Act.[15]

Though CFIUS review has become commonplace in the arena of foreign investment, the TikTok sanctions differ in that these sanctions were due to data privacy concerns. Though these types of transactions were not prevalent when CFIUS was first launched in 1975,[16] TikTok is only the latest in a procession of data privacy transactions prohibited due to national security concerns.[17] Of late, "[p]ersonal data has

---

11 Fitzpatrick, *supra* note 5, at 1088; *see also* THEODORE H. MORAN & LINDSAY OLDENSKI, FOREIGN DIRECT INVESTMENT IN THE UNITED STATES: BENEFITS, SUSPICIONS, AND RISKS WITH SPECIAL ATTENTION TO FDI FROM CHINA 55–72 (2013).

12 COMM. ON FOREIGN INV. IN THE U.S., 116TH CONG., 2019 ANNUAL REPORT TO CONGRESS 21–22 (2020).

13 Jonathan Masters & James McBride, *Foreign Investment and U.S. National Security*, COUNCIL ON FOREIGN REL. (Aug. 28, 2018), https://www.cfr.org/backgrounder/foreign-investment-and-us-national-security [https://perma.cc/H4XK-X6CX].

14 *The Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T OF TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/FY5K-PK9B] (last visited Jan. 15, 2022).

15 *See* International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1702 (1977); National Emergencies Act, 50 U.S.C. § 1601 (1976).

16 In 1975, the computer industry had just begun mass producing computers as kits to be sold for corporate and commercial use. *See generally Timeline of Computer History*, COMPUT. HIST. MUSEUM, https://www.computerhistory.org/timeline/1975/ [https://perma.cc/B7V7-GENN] (last visited Jan. 15, 2022).

17 Steven F. Hill, Michael J. O'Neil, Stacy J. Ettinger, Jeffrey Orenstein, Erica L. Bakies & Lana A. Yaghi, *Prominent Divestiture Orders Demonstrate CFIUS's Focus on Access to Sensitive Personal Data as a National Security Concern*, K&L

emerged as a mainstream concern of CFIUS."[18] To this end, the 2018 amendments to the CFIUS statutory regime include authority for Congress and the President to consider, in their investigations,[19] "[t]he extent to which a transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of U.S. citizens . . . ."[20] Critics have propounded that the "scope of 'sensitive personal data,' as defined in the proposed rule, may exceed what is necessary to protect national security."[21]

How does CFIUS define "sensitive" information? How far can this national security framework extend? Can CFIUS now review and block all transactions with a potential data privacy issue? Under the current CFIUS statute, there is no clear definition for "sensitive personal data," though the regulations do provide an infrastructure for categorizing types of data. These categories are overbroad, however, and they have essentially allowed CFIUS to review all transactions relating to data privacy, even when there were negligible or no national security issues.

GATES (May 7, 2019), https://www.klgates.com/Prominent-Divestiture-Orders-Demonstrate-CFIUSs-Focus-on-Access-to-Sensitive-Personal-Data-as-a-National-Security-Concern-05-07-2019 [https://perma.cc/2RF2-JL2V]; Jina John, *CFIUS Rule Puts National Security Spotlight on Investments that Result in Foreign Access to Sensitive Personal Data*, COOLEY (Oct. 13, 2020), https://cdp.cooley.com/cfius-rule-puts-national-security-spotlight-on-investments-that-result-in-foreign-access-to-sensitive-personal-data [https://perma.cc/VR6T-9XJT]; David Hanke & De'Siree Reeves, *CFIUS 2.0: 'Sensitive Personal Data' in the National Security Context*, JD SUPRA (Sept. 3, 2019), https://www.jdsupra.com/legalnews/cfius-2-0-sensitive-personal-data-in-91141 [https://perma.cc/FJ7Q-RZGT].

18 Carl O' Donnell, Liana B. Baker & Echo Wang, *Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, REUTERS (Mar. 27, 2020, 1:02 AM), https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-told-u-s-security-at-risk-chinese-firm-seeks-to-sell-grindr-dating-app-idUSKCN1R809L [https://perma.cc/6NNX-QZFB]; *see also* Katy Stech Ferek, *Data Privacy Increasingly a Focus of National Security Reviews*, WALL ST. J. (Sept. 14, 2020, 3:19 PM), https://www.wsj.com/articles/data-privacy-increasingly-a-focus-of-national-security-reviews-11600111141 [https://perma.cc/2J5S-KS7X].

19 U.S. DEP'T OF TREASURY, SUMMARY OF THE FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT OF 2018, https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf [https://perma.cc/K6G4-Q7SR] (last visited Feb. 18, 2022).

20 JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 13 (2020) [hereinafter JACKSON, CRS RL33388].

21 Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112, 3118 (Jan. 17, 2020) (to be codified at 31 C.F.R. pt. 800).

This Note examines the current CFIUS regime and how "national security" has necessarily expanded to include "data privacy" in light of recent CFIUS decisions and presidential sanctions. Part II will examine the current legal framework of CFIUS and how its review process has evolved over time. It discusses how the opacity of the review process and vague, broad regulations under current CFIUS legislation have contributed to CFIUS's power expanding.[22]

Part III examines the colloquial definition of national security and the lack of a clear definition of national security within the CFIUS statutory regime. Part IV looks to whether data privacy necessarily falls within the scope of national security. Next, Part V discusses how, as a matter of statutory construction, the "sensitive personal data" factor should be construed narrowly to cover some, but not all, privacy issues because only some privacy issues implicate national security. Part VI posits that, as a matter of policy, Congress should not have added the "sensitive personal data" factor because it is fundamentally different from the other types of sectors that fall within CFIUS's national security mandate. The Note contemplates the recent CFIUS decisions, comparing transactions entirely within the scope of CFIUS review based on statutory construction and policy, to those transactions which seem to have expanded CFIUS beyond its authorized parameters.

Finally, Part VII concludes by considering possible statutory and administrative changes to streamline the CFIUS process and allow for greater freedom of expression and free trade without lessening the necessary restrictions to ensure national security.

II. BRIEF OVERVIEW OF CFIUS

A. Setting

Blocking foreign transactions pertaining to data privacy concerns has recently become a mainstay on the national security docket. Since 2019, a slew of foreign transactions have been blocked by the President, CFIUS, or both due to data privacy. On August 6, 2020, the same day that President Trump ordered sanctions on TikTok, he also ordered sanctions on WeChat—a messaging, social media, and electronic payment application owned by Chinese company Tencent Holdings Ltd.—due to similar concerns of foreign ownership and mass data

22 JACKSON, CRS RL33388, *supra* note 20, at 15–16, 25, 30.

collection.[23] In 2019, CFIUS intervened and ordered Chinese gaming company Beijing Kunlun Tech Co. to divest itself of Grindr LLC, a U.S. LGBTQ+ dating application, because of its access to highly sensitive information.[24] Likewise, CFIUS ordered the Chinese investment firm iCarbonX to divest its ownership interest in PatientsLikeMe, an American start-up company geared toward providing an online forum to help medical patients find people with similar conditions.[25] In 2019, President Trump ordered the divestment of U.S. hotel software company StayNTouch from Chinese parent company Beijing Shiji Information Technology Co., claiming that the 2018 purchase "posed a national security risk."[26] Over the last few years, CFIUS has also "blocked the acquisitions of U.S. money transfer company MoneyGram International and mobile marketing firm AppLovin by Chinese bidders . . . ."[27]

Moreover, in addition to "demonstrating that personal data is a focus of national security for CFIUS, the StayNTouch, Grindr, and PatientsLikeMe transactions share an additional common thread: the parties to the respective transactions decided not to notify the

---

23 Exec. Order No. 13943, 85 Fed. Reg. 48,641 (Aug. 6, 2020) (using nearly identical language to order similar sanctions on WeChat as were placed on TikTok).

24 Sarah Bauerle Danzman & Geoffrey Gertz, *Why Is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr?*, WASH. POST (Apr. 3, 2019), https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/ [https://perma.cc/2WKA-ESG5]; *see also* Casey Newton, *How Grindr Became a National Security Issue*, VERGE (Mar. 28, 2019, 9:20 AM), https://www.theverge.com/interface/2019/3/28/18285274/grindr-national-security-cfius-china-kunlun-military [https://perma.cc/MP4V-U2UZ].

25 Christina Farr & Ari Levy, *The Trump Administration Is Forcing This Health Start-Up That Took Chinese Money into a Fire Sale*, CNBC (Apr. 4, 2019, 12:57 PM), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html [https://perma.cc/EL2E-4ZP2]; Dave Muoio, *US Regulators Forcing PatientsLikeMe's Majority Stakeholder to Divest*, MOBIHEALTHNEWS (Apr. 4, 2019, 3:16 PM), https://www.mobihealthnews.com/content/us-regulators-forcing-patientslikemes-majority-stakeholder-divest [https://perma.cc/H9FE-DURD].

26 Katy Stech Ferek, *Trump Orders Chinese Firm to Sell U.S. Hotel Software Company*, WALL ST. J. (Mar. 6, 2020, 4:49 PM), https://www.wsj.com/articles/trump-orders-chinese-firm-to-sell-u-s-hotel-software-company-11583521254 [https://perma.cc/DX3N-2493].

27 *US Pushes Chinese Owner of Grindr to Divest the Dating App: Sources*, CNBC (Mar. 27, 2019, 9:32 AM), https://www.cnbc.com/2019/03/27/us-pushes-chinese-owner-of-grindr-to-divest-the-dating-app-sources.html [https://perma.cc/L3HM-42D2].

Committee and request review."[28] While CFIUS can be initiated by the Committee's own volition or by the parties' voluntary notice, commentators in the past claimed that "in practice . . . , CFIUS has not initiated reviews but has instead encouraged parties to not-yet-notified sensitive transactions to file a notice voluntarily."[29] CFIUS, however, has now initiated review of non-notified transactions as well, extending the discretion it has been granted to its outer limits and ramping up its enforcement techniques.[30]

The TikTok sanctions, along with other recent data related CFIUS activity, demonstrate the lack of clarity as to the general scope and authorization of CFIUS power under the current CFIUS legislation. With the rapid increase in globalization and the sheer volume of FDI, the lack of sufficient national security guidance can lead to a detrimental reduction of FDI.

B. Background

1. Early CFIUS

Before CFIUS, little could be done about foreign-owned companies operating or seeking to operate in the United States. The President's authority was considered "an extremely blunt instrument."[31] The Trading with the Enemy Act ("TWEA"), enacted by Congress in 1917, granted the President the power to oversee and restrict all trade

---

28 Steven F. Hill, Stacy J. Ettinger, Michael J. O'Neil, Jeffrey Orenstein, Erica L Bakies & Sarah F. Burgart, *Recent Actions by CFIUS Underscore Importance of Review Process*, K&L GATES (Mar. 20, 2020), https://www.klgates.com/Recent-Actions-By-CFIUS-Underscore-Importance-of-Review-Process-03-20-2020 [https://perma.cc/NJF9-PG3M].

29 George Stephanov Georgiev, Comment, *The Reformed CFIUS Regulatory Framework: Mediating Between Continued Openness to Foreign Investment and National Security*, 25 YALE J. REG. 125, 127 (2008); *see* U.S. GOV'T ACCOUNTABILITY OFF., GAO-05-686, ENHANCEMENTS TO THE IMPLEMENTATION OF EXON-FLORIO COULD STRENGTHEN THE LAW'S EFFECTIVENESS 2, 7 (2005).

30 Hill, Ettinger, O'Neil, Orenstein, Bakies & Burgart, *supra* note 28 ("CFIUS recently indicated that it continues to add resources toward, and place importance on, review of non-notified transactions that present national security concerns."); *see also* James Brower, Amy Josselyn, Richard Matheny III, Jacob Osborn & Justin Pierce, *When Your Investment Is Rockin' and CFIUS Comes A-Knockin': The CFIUS Non-Notified Process*, JD SUPRA (Feb. 4, 2021), https://www.jdsupra.com/legalnews/when-your-investment-is-rockin-and-8379385 [https://perma.cc/B9YH-CWYK].

31 David Zaring, *CFIUS as a Congressional Notification Service*, 83 S. CAL. L. REV. 81, 91 (2010).

between the United States and its enemies, but only in times of war.[32] Additionally, in response to the Vietnam War, Congress enacted the IEEPA, authorizing the President "to deal with any unusual and extraordinary threat . . . to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat."[33] As such, the TWEA was to be used strictly in wartime, while the IEEPA was for the President to use during times of peace. While "[t]hese powers were real, . . . it was not clear whether a troubling merger would qualify as a sufficient national emergency trigger to allow the president to exercise them."[34]

This ambiguity remained unresolved until after the 1973 oil embargo when "oil-rich investors" sought to "invest in American assets."[35] Congress was concerned that a substantial portion of the "huge petrodollar surplus" obtained by the Organization of Petroleum Exporting Countries ("OPEC") during the embargo would be "return[ed] in the form of direct investment" into U.S. companies.[36] In response, on May 7, 1975, a worried President Ford established a committee, known as CFIUS, via executive order to monitor whether foreign interests should be allowed to purchase American assets.[37] The executive order gave CFIUS "primary continuing responsibility within the Executive Branch for monitoring the impact of foreign investment in the United States . . . ."[38] It directed CFIUS to:

> (1) arrange for the preparation of analyses of trends and significant developments in foreign investment in the United States;

---

32 Trading with the Enemy Act, Pub. L. No. 65-91, § 5, 40 Stat. 411, 415 (1917).

33 International Emergency Economic Powers Act, 50 U.S.C. § 1701(a).

34 Zaring, *supra* note 31, at 91.

35 *Id.* at 91–92; *Oil Embargo, 1973–1974*, U.S. DEP'T OF STATE OFF. OF THE HISTORIAN, https://history.state.gov/milestones/1969-1976/oil-embargo#:~:text=During%20the%201973%20Arab%2DIsraeli,the%20post%2Dwar%20peace%20negotiations. [https://perma.cc/8W4U-RWLJ] (last visited Jan. 15, 2020).

36 Zaring, *supra* note 31, at 92 (quoting C.S. Eliot Kang, *U.S. Politics and Greater Regulation of Inward Foreign Direct Investment*, 51 INT'L ORG. 301, 302 (1997)); *see also* Patrick Griffin, Note, *CFIUS in the Age of Chinese Investment*, 85 FORDHAM L. REV. 1757, 1762 (2017) ("At the time, many in Congress feared that, in light of the oil embargo launched by OPEC two years earlier, the spurt of investment was motivated by political rather than economic considerations.").

37 Exec. Order No. 11858, 3 C.F.R. § 990 (1971–1975).

38 *Id.* § 991.

> (2) provide guidance on arrangements with foreign governments for advance consultations on prospective major foreign governmental investment in the United States;
>
> (3) review investment in the United States which, in the judgment of the Committee, might have major implications for United States national interests; [and]
>
> (4) consider proposals for new legislation or regulations relating to foreign investment as may appear necessary.[39]

Between 1975 and 1980, CFIUS was effectively silent, only meeting a handful of times and "never conclud[ing] that a prospective acquisition required any Federal intervention."[40] Critics claim that CFIUS was paralyzed by its inability "to decide whether it should respond to the political or the economic aspects of [FDI] in the United States."[41] During a 1979 congressional hearing, a critic claimed that CFIUS incorrectly focused only on the politics of certain transactions, instead of simply asking "[i]s it good for the economy?"[42] Thus began CFIUS's consistent battle with conflicting approaches of "taking a passive, investment-friendly approach to review" versus a litigious, "advocating of a more protectionist stance."[43]

In the 1980s, at the behest of the Department of Defense, CFIUS investigated a few foreign transactions, becoming more active.[44] The result of these reviews was either that the foreign firm would withdraw potential offers to acquire American companies, or, conversely, acquisitions would be completed so long as production of the good was maintained wholly in the United States or so long as the acquisition was reassigned to a U.S. parent company.[45]

2. Exon-Florio Amendment

It was not until 1988 that congress was spurred into altering foreign investment policy once more. Japanese firm Fujitsu Ltd. made an

---

39 *Id.*

40 135 CONG. REC. H5334 (1989) (statement of Rep. Wolf); *see* JACKSON, CRS RL33388, *supra* note 20, at 3.

41 JACKSON, CRS RL33388, *supra* note 20, at 3 (citing H.R. REP. NO. 96-1216, at 166–84 (1980)).

42 *Id.* (citing *The Operations of Federal Agencies in Monitoring, Reporting on, and Analyzing Foreign Investments in the United States: Hearing Before the Subcomm. on Com., Consumer, & Monetary Affs. of the H. Comm. on Gov't Operations*, 96th Cong. 5 (1979)).

43 Griffin, *supra* note 36, at 1763.

44 JACKSON, CRS RL33388, *supra* note 20, at 3.

45 *Id.* at 6–7.

offer to acquire eighty percent of Fairchild Semiconductor Co., a California firm in the business of making semi-conductors owned by Shlumberger Ltd. of France.[46] Congress thought that the potential acquisition would "damage U.S. competitiveness and harm national security by giving Japan access to vital U.S. technology and making the United States dependent on Japan for semiconductor production."[47] Moreover, the Department of Defense was alarmed that the sale would lead to foreign control of a major American supplier of computer chips to the military, weakening U.S. defense industries.[48]

At the time, CFIUS essentially only retained powers of review with no real powers of enforcement.[49] As such, the only recourse the United States had under its then-existing foreign investment policy was for the President to invoke the IEEPA,[50] which "would have been seen as an overtly hostile act against Japan."[51] In a bout of protectionist unease at the possibility of Japanese firms acquiring American companies, Congress hastily sought to codify CFIUS's ability to review foreign investment.[52]

Congress passed the Omnibus Foreign Trade and Competitiveness Act of 1988, which contains the Exon-Florio Amendment ("Exon-Florio") to the Defense Production Act.[53] Under the Act, the President has the authority to block foreign "mergers, acquisitions, and takeovers" of "persons engaged in interstate commerce" that

---

46 Donna K. H. Walters, *Deal to Sell Fairchild Semiconductor to Fujitsu Canceled*, L.A. TIMES (Mar. 17, 1987), https://www.latimes.com/archives/la-xpm-1987-03-17-fi-12290-story.html [https://perma.cc/EJR5-CT3B]; Michael Schrage, *Fuitsu Buying Stake in Fairchild*, WASH. POST (Oct. 25, 1986), https://www.washingtonpost.com/archive/business/1986/10/25/fuitsu-buying-stake-in-fairchild/ac93a960-71bf-4b0f-a5b6-9faddc389114 [https://perma.cc/FA8N-MCU2].

47 Griffin, *supra* note 36, at 1763.

48 Stuart Auerbach, *Cabinet to Weigh Sale of Chip Firm*, WASH. POST (Mar. 12, 1987), https://www.washingtonpost.com/archive/business/1987/03/12/cabinet-to-weigh-sale-of-chip-firm/63c934e8-0393-43eb-9ca2-a2ccd1d926fe/?utm_term=.1aee86fa55d0 [https://perma.cc/FH7H-YVY9].

49 *See* Exec. Order No. 11858, 3 C.F.R. § 991 (1971–1975) (authorizing CFIUS to review any deal with potential "major implications for United States national interests" but not actually granting any actual power to ensure its recommendations were fulfilled).

50 *See* International Emergency Economic Powers Act, 50 U.S.C. § 1701.

51 Griffin, *supra* note 36, at 1764.

52 *See* H.R. 4848, 100th Cong. (1988).

53 Omnibus Foreign Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, 102 Stat. 1107, 1425–26 (codified as amended at 50 U.S.C. app. §§ 2158–2170 (2000)).

threatens to impair the national security.[54] The Act, however, curtails the President's power by allowing him to exercise this power only after concluding that: (1) other U.S. laws are inadequate or inappropriate to protect the national security, and (2) "credible evidence" exists demonstrating that "the foreign interest exercising control might take action that threatens to impair [U.S.] national security."[55] In fact, "[p]rior to [Exon-Florio], foreign acquisitions could be blocked only if the President declared a national emergency or regulators found a violation of federal antitrust, environmental, or securities laws."[56]

Under Exon-Florio, CFIUS has to consider the following factors in deciding whether a foreign transaction implicates national security concerns: (1) the effect of the proposed acquisition on U.S. production capacity in areas relevant to national security; (2) the potential effects of the transaction on U.S. technological leadership in areas affecting U.S. national security; (3) the potential national security effects on U.S. critical infrastructure, including major energy assets; (4) whether the covered transaction is a foreign-government-controlled transaction; (5) the state of relations between the company's country and the United States, specifically with respect to cooperating in counterterrorism efforts; (6) the long-term projection of U.S. requirements for sources of energy and other critical resources; and (7) such other factors as the President or the Committee may determine to be appropriate.[57]

In enacting the Omnibus Foreign Trade and Competitiveness Act, one of the most hotly contested issues was the definition of national security.[58] The Reagan Administration advocated for language that would broaden the scope of national security, arguing that "national security and essential commerce" should include "a strong economic component" within its definition.[59] The words "essential commerce," believed to be too expansive, were ultimately stricken from the final language.[60] At the time, "Treasury Department officials . . . indicated . . . that during a review or investigation each member of CFIUS is expected to apply that definition of national security that is consistent

54 § 721, 102 Stat. at 1425.

55 § 721, 102 Stat. at 1426.

56 Georgiev, *supra* note 29, at 127.

57 50 U.S.C. § 4565(f).

58 JACKSON, CRS RL33388, *supra* note 20, at 7 ("Of these issues, the most controversial and far-reaching was the lack of a definition of national security.").

59 *Id.*

60 *Id.*

with the representative agency's specific legislative mandate."[61] This approach—an incoherent attempt to establish a designation for the term—may very well be the source of much confusion and arguably a wrongful expansion of CFIUS review.

Of paramount importance to the evolution of CFIUS, President Reagan issued an executive order that delegated his initial review and decision-making responsibilities to CFIUS.[62] This order transformed "an administrative body with limited authority to review and analyze data on foreign investment to an important component of U.S. foreign investment policy with a broad mandate and significant authority to advise the President on foreign investment transactions and to recommend that some transactions be suspended or blocked."[63]

3. The Byrd Amendment

Though Exon-Florio provided CFIUS with a broad grant of authority, in the years following, CFIUS only investigated sixteen transactions, blocking just one.[64] Therefore, in 1992, Congress amended Exon-Florio through Section 837(a) of the National Defense Authorization Act for Fiscal Year 1993.[65] Known as the Byrd Amendment, after Senator Robert Byrd, this amendment made several noteworthy changes. First, CFIUS was now required to carry out *mandatory* investigations of mergers, acquisitions, and takeovers where the acquirer is "controlled by or acting on behalf of a foreign government" and 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."[66] The amendment also supplemented the review process with specific factors to consider in blocking an acquisition, such

61 JAMES K. JACKSON, CONG. RSCH. SERV., RS22863, FOREIGN INVESTMENT, CFIUS, AND HOMELAND SECURITY: AN OVERVIEW 2 (2011) [hereinafter JACKSON, CRS RS22863]; *see generally* JAMES K. JACKSON, CONG. RSCH. SERV., RL33312, THE EXON-FLORIO NATIONAL SECURITY TEST FOR FOREIGN INVESTMENT 7 (2013) [hereinafter JACKSON, CRS RL33312].

62 Exec. Order No. 1266, 54 Fed. Reg. 779 (Dec. 27, 1988).

63 JACKSON, CRS RL33388, *supra* note 20, at 8.

64 Robert Shearer, Comment, *The Exon-Florio Amendment: Protectionist Legislation Susceptible to Abuse*, 30 HOUS. L. REV. 1729, 1754–66 (1993) (discussing some of the paltry investigations conducted by CFIUS following Exon-Florio's enactment).

65 National Defense Authorization Act for Fiscal Year 1993, Pub. L. No. 102-484, 106 Stat. 2315 (codified as amended in scattered sections of 10 U.S.C.).

66 *Id.* § 837(a), 106 Stat. at 2464.

as whether the country had a history of cooperation with counter-terrorism efforts and adherence to nonproliferation control regimes.[67]

In 2006, CFIUS refused to conduct a forty-five-day investigation into DP World's acquisition of a U.S. company by a United Arab Emirates state-owned corporation, Dubai Ports World.[68] This led to tensions between CFIUS and Congress. CFIUS argued that based on its extensive informal prereview investigation, the deal did not pose a national security threat and thus did not meet the second criterion of the Byrd Amendment.[69] Congress, concerned with the aftermath of the terrorist attacks on September 11, 2001, was hesitant of Middle Eastern acquisitions and vehemently disputed CFIUS's decision, leading President Bush to once again alter the manner in which CFIUS reviewed foreign transactions.[70] Thus, CFIUS and President Bush approved the acquisition of Lucent Technologies, Inc. by French corporation, Alcatel S.A., but only after Alcatel signed a Special Security Arrangement restricting its access to sensitive work done by Lucent pertaining to the United States' communications infrastructure, and with the stipulation that CFIUS could reopen a review of the deal and overturn approval at any point.[71] This event layered the already arguably opaque CFIUS review process with greater uncertainty since foreign investors could no longer feel settled once their deals passed CFIUS muster, as CFIUS retained the right to reopen any investigations.

4. The Foreign Investment and National Security Act of 2007

In 2007, in response to CFIUS's persistent inaction, Congress enacted the Foreign Investment and National Security Act of 2007 ("FINSA").[72] Before 2007, CFIUS's authority had only been defined

---

67 *Id.* § 837(b), 106 Stat. at 2464; *see also* 50 U.S.C. app. § 2170(b)(4)(A)(i)–(iii).

68 *See* JACKSON, CRS RL33388, *supra* note 20, at 4.

69 *See id.* at 9.

70 *See id.*

71 *See id.* at 9–10.

72 Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246 (amending 50 U.S.C. app. §§ 2158–2170 (2000)); Press Release, Off. of the Press Sec'y, President Bush Signs Foreign Investment and National Security Act of 2007 (July 26, 2007), https://georgewbush-whitehouse.archives.gov/news/releases/2007/07/20070726-6.html [https://perma.cc/HHK8-LG88]; Exec. Order No. 13456, 73 Fed. Reg. 4,677 (Jan. 23, 2008).

by a series of executive orders,[73] but FINSA made several changes. FINSA made CFIUS official by finally giving the Committee statutory authority;[74] allotted the Committee specified times for the review process (thirty days to conduct an initial review, forty-five days to conduct an investigation if the review gave rise to national security concerns, and fifteen days for the President to make a final decision);[75] allowed for an informal review process, which normally occurs prior to filing a transaction with CFIUS and allows individual companies to privately discuss and correct any issues with their transaction;[76] and added more factors in addition to those which CFIUS was already obliged to consider under previous iterations of this statute.[77]

---

73 Exec. Order No. 11858, 3 C.F.R. § 990 (1971–1975), *as amended by* Exec. Order No. 12188, 45 Fed. Reg. 989 (Jan. 2, 1980); Exec. Order No. 12661, 54 Fed. Reg. 779 (Dec. 27, 1988); Exec. Order No. 12860, 58 Fed. Reg. 47,201 (Sept. 3, 1993); Exec. Order No. 13286, 68 Fed. Reg. 10,619 (Feb. 28, 2003).

74 JACKSON, CRS RL33388, *supra* note 20, at 10.

75 *Id.*; *see also* JACKSON, CRS RL33312, *supra* note 61, at 9.

76 JACKSON, CRS RL33388, *supra* note 20, at 11.

77 The list of eleven factors that the President must consider and CFIUS may consider in their investigations includes:

> (1) domestic production needed for projected national defense requirements;
>
> (2) capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services;
>
> (3) control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security;
>
> (4) the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country–
>
> (A) identified by the Secretary of State–
>
> (i) . . . as a country that supports terrorism;
>
> (ii) . . . as a country of concern regarding missile proliferation; or
>
> (iii) . . . as a country of concern regarding the proliferation of chemical and biological weapons;
>
> (B) identified by the Secretary of Defense as posing a potential regional military threat to the interests of the United States; or
>
> (C) listed under section 309(c) of the Nuclear Non-Proliferation Act of 1978 . . . on the "Nuclear Non-Proliferation-Special Country List" . . . or any successor list;
>
> (5) the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security;
>
> (6) the potential national security-related effects on United States critical infrastructure, including major energy assets;
>
> (7) the potential national security-related effects on United States critical technologies;

5. Foreign Investment Risk Review Modernization Act

In 2017, Congress became concerned about the extent of China's growing investment in the United States. As such, CFIUS authority was further extended pursuant to the 2018 Foreign Investment Risk Review Modernization Act ("FIRRMA").[78] FIRRMA expanded the scope and jurisdiction of CFIUS by redefining "covered transactions," adding four new types of covered transactions: (1) "the purchase or lease by, or a concession to, a foreign person of certain private or public real estate" located in proximity to sensitive government facilities; (2) "other investments" in certain U.S. businesses that afford a foreign person "access to any material nonpublic technical information in the possession of the target U.S. business," membership on the board of directors, or other decision-making rights, other than through voting of shares; (3) any change in a foreign investor's rights resulting in foreign control of a U.S. business or an "other investment" in certain U.S.

> (8) whether the covered transaction is a foreign government-controlled transaction . . .;
> (9) as appropriate . . ., a review of the current assessment of–
> (A) the adherence of the subject country to nonproliferation control regimes, including treaties and multilateral supply guidelines, which shall draw on, but not be limited to, the annual report on 'Adherence to and Compliance with Arms Control, Nonproliferation and Disarmament Agreements and Commitments' required by section 403 of the Arms Control and Disarmament Act [22 U.S.C. [§] 2593a];
> (B) the relationship of such country with the United States, specifically on its record on cooperating in counter-terrorism efforts, which shall draw on, but not be limited to, the report of the President to Congress under section 7120 of the Intelligence Reform and Terrorism Prevention Act of 2004; and
> (C) the potential for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations;
> (11) the long-term projection of United States requirements for sources of energy and other critical resources and materials; and
> (12) such other factors as the President or the Committee may determine to be appropriate . . ..

50 U.S.C. app. § 2170(f); Foreign Investment and National Security Act of 2007 § 4, 121 Stat. at 253 (adding factors 6–12 and section (C) of factor 4).

78 Foreign Investment Risk Review Modernization Act of 2018, 50 U.S.C. § 4565; *see also* Rachel H. Boyd, *FIRRMA: "Buy American" Products, or Bye American Progress?*, 19 WAKE FOREST J. BUS. & INTELL. PROP. L. 103, 106 (2019) ("However, FINSA did not broaden the CFIUS jurisdictional scope to the extent the Trump administration believed was necessary to address national security concerns, which ultimately led to the enactment of FIRRMA.").

businesses; and (4) "any other transaction, transfer, agreement, or arrangement, designed or intended to circumvent" CFIUS jurisdiction.[79]

Under FIRRMA, CFIUS's review authority was expanded to include not only foreign takeovers and mergers for controlling interests of U.S. businesses, but also for non-controlling interests of or access rights to businesses of special concern, namely, critical technology, critical infrastructure, and sensitive personal data (known in the regulations as "T.I.D. U.S. Businesses").[80] Specifically with regard to data-related businesses, FIRRMA delineated that CFIUS must review transactions for "[a]ny other investment" which "maintains or collects *sensitive personal data* of United States citizens that may be exploited in a manner that threatens national security."[81] For transactions regarding non-controlling foreign interests in investments, CFIUS can review "other investments" involving "the use, development, acquisition, safekeeping, or release of *sensitive personal data* of United States citizens maintained or collected by the United States business."[82]

Additionally, FIRRMA extended CFIUS's timelines, expanding their thirty-day review period to forty-five days, and even allowing for an extra fifteen-day extension under extraordinary circumstances.[83] FIRRMA defined "critical technologies," and "critical infrastructure," and strengthened requirements on the use of mitigation agreements, including the addition of compliance plans and pilot programs, which allow for CFIUS to expand its power by "conduct[ing] pilot programs to implement provisions in the legislation that did not become effective immediately upon enactment."[84] Moreover, on October 15, 2020, FIRRMA provided for mandatory "declarations" or filings for transactions in which the foreign government has a "substantial interest"

---

79 JACKSON, CRS RL33388, *supra* note 20, at 20–21.

80 31 C.F.R. § 800.248 (2021).

81 50 U.S.C. § 4565(a)(4)(B)(iii)(III) (2021) (emphasis added).

82 *Id.* § 4565(a)(4)(D)(i)(III)(aa) (emphasis added).

83 *Id.*; *see* Christopher M. Tipler, *Defining 'National Security': Resolving Ambiguity in the CFIUS Regulations*, 35 U. PA. J. INT'L L. 1223, 1256 (2014) (arguing that the CFIUS timeline of ninety days under FINSA is too long and decreases the value of cross-border deals since time is critical to the value of cross-border deals, as they can be "expose[d] . . . to many risks, particularly in the volatile international business context" and the "potential to make the deal no longer profitable or desirable."). If critics took issue with a ninety-day timeline, then the new 105-day process, and possibly 120-day process, under FIRRMA could only serve to heighten the concern that deals will be exposed to risk for longer, decreasing the value ten-fold.

84 Press Release, U.S. Dep't of the Treas., Treasury Releases Interim Regulations for FIRRMA Pilot Program (Oct. 10, 2018).

and allows CFIUS to establish such declarations for other "critical technology" transactions as well.[85]

In essence, FIRRMA was enacted as an expansive protective measure,[86] and as such, many commentators have referred to it as the "most significant overhaul of the agency's powers since 1988."[87] Skeptics at the time claimed that FIRRMA would "overburden CFIUS, hamper the competitiveness of U.S. companies, and dampen the dynamism of the technology sector."[88]

To this effect, Congress inputted a "Sense of Congress" provision, adding more factors that the President and CFIUS *may* consider in investigating a foreign transaction, including: (1) whether the covered transaction involves a country of special concern;[89] (2) the potential effects of the cumulative control of or pattern of recent transactions with any one type of critical infrastructure or energy asset;[90] (3) whether the foreign person involved in the transaction has a history of compliance with U.S. laws and regulations;[91] (4) the control of U.S. industries and commercial activity that affect U.S. capability to meet national security requirements;[92] (5) "the extent to which a covered transaction is likely to expose, either directly or indirectly, personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that *may exploit that information in a manner that threatens national security*";[93] and (6) whether a transaction "is likely to exacerbate or create new cybersecurity vulnerabilities or is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities."[94] While helpful for CFIUS

---

85 Farhad Jalinous, Karalyn Mildorf, Keith Schomig & Cristina Brayton-Lewis, *CFIUS Reform Becomes Law: What FIRRMA Means for Industry*, WHITE & CASE (Aug. 13, 2018), https://www.whitecase.com/publications/alert/cfius-reform-becomes-law-what-firrma-means-industry [https://perma.cc/SW36-QGXU].

86 Boyd, *supra* note 78, at 107.

87 Masters & McBride, *supra* note 13; *see also* Samuel Rubenfeld, *The Morning Risk Report: CFIUS Reform Becomes Law*, WALL ST. J. (Aug. 15, 2018, 9:23 AM), https://www.wsj.com/articles/the-morning-risk-report-cfius-reform-becomes-law-1534339391?tesla=y [https://perma.cc/4HGU-C9BU].

88 Masters & McBride, *supra* note 13.

89 Foreign Investment Risk Review Modernization Act of 2018, 50 U.S.C. § 4565(f)(4).

90 *Id.* § 4565(f)(6).

91 *Id.* § 4565(f)(7).

92 *Id.* § 4565(f)(5).

93 JACKSON, CRS RL33388, *supra* note 20, at 31 (emphasis added).

94 *Id.* at 13.

review, ultimately these factors, which comprise a concurrent Congressional resolution, have "no formal effect on public policy and have no force of law."[95]

Thus, while "FIRRMA provides the general contours for CFIUS reform," it does not provide the specifics, and "[t]o achieve broad-based support for FIRRMA . . . , many of the novel, difficult, or contentious issues were deferred to the regulation-writing process."[96] The Department of the Treasury emphasized that the FIRRMA restrictions were drafted to provide as much clarity and specificity as possible to businesses.[97] However, the Committee merely defined "sensitive personal data" as data that *may* be exploited to threaten national security.[98] Many organizations took issue with the CFIUS reforms, specifically with regard to the sensitive personal data provision.[99] Biotech companies with access to genetic information vied that they be removed from the list of industries with mandatory declarations, while "other companies requested that sensitive personal data be tailored to actual national security risks, positing that the current formulation is overbroad."[100]

a. "Sensitive Personal Data"

In response to these critiques, the final regulations defined "sensitive personal data" by dividing it into two classes of information: (1) identifiable data that (i) has been collected by U.S. businesses fulfilling certain requirements, and (ii) are categorically identifiable

---

95 CHRISTOPHER M. DAVIS, CONG. RSCH. SERV., R98-825, "SENSE OF" RESOLUTIONS AND PROVISIONS 2 (2019).

96 Farhad Jalinous, Karalyn Mildorf, Keith Schomig & Ata Akiner, *CFIUS Finalizes New FIRRMA Regulations*, WHITE & CASE (Jan. 22, 2020), https://www.whitecase.com/publications/alert/cfius-finalizes-new-firrma-regulations [https://perma.cc/T7K5-9JWV] ("FIRRMA contains no definitions or delineating principles with respect to 'sensitive personal data,' other than that it refers to data that may be exploited in a manner that threatens national security."); *see also* 50 U.S.C. § 4565(a)(4)(D)(iii)(I) ("The Committee shall prescribe regulations providing guidance on the types of transactions that the Committee considers to be 'other investment' for purposes of subparagraph (B)(iii).").

97 Jalinous, Mildorf, Schomig & Brayton-Lewis, *supra* note 85.

98 *Fact Sheet: Proposed CFIUS Regulations to Implement FIRRMA*, DEP'T OF TREASURY 3 (Sept. 17, 2019), https://home.treasury.gov/system/files/206/Proposed-FIRRMA-Regulations-FACT-SHEET.pdf [https://perma.cc/J8D7-B8HE].

99 Antonia I. Tzinova, *New CFIUS Regulations Finally Take Effect*, HOLLAND & KNIGHT (Feb. 13, 2020), https://www.hklaw.com/en/insights/publications/2020/02/new-cfius-regulations-finally-take-effect [https://perma.cc/X6ZV-Y6C7].

100 *Id.*

within the ten categories of data set forth by the regulations; and (2) results of an individual's genetic tests, including genetic sequencing data, whenever those results constitute identifiable data.[101]

b. Identifiable Data

To constitute identifiable data, the first class of "sensitive personal data" defined under the regulations, the data must be maintained or collected by U.S. businesses that (i) "target[] or tailor[]" products or services to U.S. government personnel, such as "any U.S. executive branch agency or military department with intelligence, national security, or homeland security responsibilities, or to personnel and contractors thereof"; (ii) maintain or collect data on more than one million individuals; or (iii) have a "demonstrated business objective to maintain or collect data" on more than one million individuals as part of its primary product or service.[102]

The regulations also state that identifiable data must come from one of the following ten categories of data maintained or collected by U.S. businesses: (1) data "used to analyze or determine an individual's financial distress or hardship"; (2) "[t]he set of data in a consumer report . . ."; (3) the set of data in an application for health insurance, long-term care insurance, professional liability insurance, mortgage insurance, or life insurance; (4) "[d]ata relating to the physical, mental, or psychological health condition of an individual"; (5) "[n]on-public electronic communications, including email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications"; (6) "[g]eolocation data collected using positioning systems, cell phone towers, or WiFi access points such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device"; (7) "[b]iometric enrollment data including facial, voice, retina/iris, and palm/fingerprint templates"; (8) "[d]ata stored and processed for generating a state or federal government identification card"; (9) "[d]ata concerning U.S. Government personnel security clearance status"; or (10) "[t]he set of

101 31 C.F.R. § 800.241(a)(1)–(2) (2021) ("Such results shall not include data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research. For purposes of this paragraph, 'genetic test' shall have the meaning provided in 42 U.S.C. [§] 300gg-91(d)(17).").

102 *Id.* § 800.241(a)(1)(i)(A)–(C).

data in an application for a U.S. Government personnel security clearance or an application for employment in a position of public trust."[103]

c. Genetic Information

Moreover, the regulations narrow the scope of genetic information which qualifies as sensitive personal data by (1) refocusing the definition on "genetic tests" as defined in the Genetic Information Non-Discrimination Act of 2020 ("GINA") and (2) limiting the coverage to identifiable data.[104] As such, a genetic test is defined as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes" and does not include "an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved."[105] A key exception to note is that "a company may maintain one or all of the enumerated categories of personal data but still fall outside of the scope of CFIUS investment review if it does not specifically target government employees or does not meet the one million person threshold."[106] However, genetic information, which is particularly sensitive, is exempt from these limitations.[107]

C. Issues with CFIUS Legislation

1. Broad Vague Sensitive Data Regulations

The regulations on CFIUS's sensitive data factor have been referred to as "complex and broad."[108] In fact, critics have argued that

---

103 *Id.* § 800.241(a)(1)(ii)(A)–(J).

104 *Id.* § 800.241(a)(2); *see also* David Mortlock, Noman Goheer, Ahmad El-Gamal, *Expanded CFIUS Jurisdiction Under FIRRMA Regulations: An Overview*, at 6, Willkie.com, https://www.willkie.com/-/media/files/publications/2020/05/expandedcfiusjurisdictionunderfirrmaregulations.pdf (last visited Mar. 11, 2022).

105 42 U.S.C. § 300gg-91(d)(17)(A), (d)(17)(B)(ii).

106 Austin Mooney, *Spotlight on Sensitive Personal Data as Foreign Investment Rules Take Force*, NAT'L L. REV. (Feb. 18, 2020), https://www.natlawreview.com/article/spotlight-sensitive-personal-data-foreign-investment-rules-take-force [https://perma.cc/F5P7-8ZEZ].

107 31 C.F.R. § 800.241(a)(2).

108 Martin Chorzempa, *New CFIUS Regulations: More Powerful, Transparent, and Complex*, PIIE (Oct. 10, 2019, 11:15 AM), https://www.piie.com/blogs/trade-and-investment-policy-watch/new-cfius-regulations-more-powerful-transparent-and-complex [https://perma.cc/3DFF-P6ZG].

"the data rules as proposed could overload CFIUS's limited manpower with filings of little relevance to national security, reducing its ability to focus on the most serious cases."[109] The regulations attempted to limit CFIUS's mandate by defining sensitive data as "identifiable," ruling out anonymized data, data on one's own employees, data from companies that occasionally do credit checks, and cloud storage providers where data is encrypted and the company is unable to decrypt it.[110] The rule even specifies that "simply having emails or chats does not qualify as sensitive data. They qualify only if the 'primary purpose of such product or service is to facilitate third-party user communications.'"[111] However, "[d]espite these apparent narrow definitions of what constitutes sensitive data," commentators correctly foreshadowed that "the impact will nevertheless be widespread" due to the low threshold requirement of one million individuals, which includes non-U.S. citizens.[112]

III. DEFINING NATIONAL SECURITY IN CFIUS CASES

What is "national security"? Wherever this term has been raised in American jurisprudence, even preceding the CFIUS context, the definition has been hazy at best.[113] National security has colloquially been understood as "the safeguarding of a people, territory, and way of life," which "encompasses the protection of the fundamental values and core interests necessary to the continued existence and vitality of the state."[114] As such, any congressional or presidential decision made with respect to national security concerns, particularly those including

109 *Id.*

110 *Id.*

111 *Id.* at n.2.

112 *Id.*

113 *See* Paton v. La Prade, 469 F. Supp. 773, 774 (D.N.J. 1978) (holding that a postal regulation authorizing mail covers, which consist of a process whereby a record is made of any data appearing on the outside cover of any class of mail matter, to "protect the national security" is unconstitutionally vague and overbroad); *see also* Zweibon v. Mitchell, 516 F.2d 594, 636 n.108 (D.C. Cir. 1975) (in discussing the potential constitutional questions implicated by allowing warrantless surveillance by wiretap of a domestic organization via presidential order, the United States District Court for the District of Columbia explained that "the tendency has been to give the term 'national security' an overly broad definition." Moreover, the court went on to add, "the exception . . . is not limited to 'national security' wiretapping in its traditional sense, but extends to *any* information which 'affects' foreign affairs or which may be of use in formulating foreign policy decisions").

114 AMOS A. JORDAN, WILLIAM J. TAYLOR JR., MICHAEL J. MEESE, SUZANNE C. NIELSEN & JAMES SCHLESINGER, AMERICAN NATIONAL SECURITY 3–4 (6th ed. 2009).

"fundamental values" or "core interests," may entail, to some extent, a policy determination of foreign political frameworks and their goals.[115] Moreover, national security has been described as "a prophylactic concept, concerned with potential dangers—with 'intangibles, uncertainties and probabilities rather than [with] concrete threats readily foreseeable and easily grasped.'"[116] The precise concept is quite difficult to contract into one single conception.

"Despite its appearance throughout history and its use in relation to statutory authorities . . . , 'national security' is rarely defined."[117] In fact, the National Security Act of 1947, the Foreign Intelligence Surveillance Act of 1978, and the 2001 Omnibus Patriot Act all refer to "national security" numerous times without actually defining it.[118] Likewise, Congress has refused to corral national security into one coherent definition for the purpose of CFIUS review.[119] Under the regulations, each CFIUS member is expected to apply the definition "consistent with the representative agency's legislative mandate."[120]

---

115 Robert C. Post, Note, *National Security and the Amended Freedom of Information Act*, 85 YALE L.J. 401, 411 (1976).

116 *Id.* (quoting Charles L. Schultze, *The Economic Content of National Security Policy*, 51 FOREIGN AFF. 522, 530 (1973)).

117 Laura K. Donahue, *The Limits of National Security*, 48 AM. CRIM. L. REV. 1573, 1579 (2011).

118 *Id.*

119 JACKSON, CRS RL33388, *supra* note 20, at 13; *see* Theodore H. Moran, *CFIUS and National Security: Challenges for the United States, Opportunities for the European Union* 5 (Peterson Inst. Int'l Econ. 2017), https://www.piie.com/system/files/documents/moran201702draft-c.pdf [https://perma.cc/ECV8-LGEW] (explaining that FINSA, like earlier CFIUS regulations, left "the definition of national security [] not explicitly defined . . . ."); *see also* Tipler, *supra* note 83, at 1242 (discussing how because the regulations failed to define "national security," FINSA directed that the Committee publish guidance in the Federal Register); *see generally* Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74567, 74568 (Dec. 8, 2008) [hereinafter Guidance] ("The guidance is issued pursuant to section 721(b)(2)(E), which requires the Chairperson of the Committee on Foreign Investment in the United States to publish guidance regarding the types of transactions that it has reviewed and that have presented national security considerations."). However, the Guidance itself states that it "does not provide comprehensive guidance on all types of covered transactions that have presented national security considerations." *Id.* at 74570.

120 JACKSON, CRS RS22863, *supra* note 61, at 13 (citing *Briefing by Representatives from the Departments and Agencies Represented on the Committee on Foreign Investment in the United States (CFIUS) to Discuss the National Security Implications of the Acquisition of Peninsular and Oriental Steamship Navigation Company by Dubai Ports World, a Government-Owned and -Controlled Firm of the United Arab Emirates (UAE): Hearing Before the S. Comm. on Armed Serv.*, 109th Cong. (2006)).

Perhaps it is a purposeful choice to leave the term open-ended to empower CFIUS for a broader reach of review of any FDI in uncharted territory that may be contemplated as problematic vis a vis this notion of national security.[121] However, implementing a regulatory framework for handling national security concerns without a working definition of national security is wholly unhelpful, akin to trying to collect water in a cracked vessel. This vagueness causes an absence of limitation, where CFIUS members can each introduce differing and arbitrary definitions of national security that haphazardly narrow or broaden the scope of CFIUS review.[122] Since the concept itself is difficult to pin down, allowing for conflicting opinions and definitions can only further complicate the CFIUS process. A recent research report written on CFIUS explains how the Committee is still figuring out a "working set of parameters that establish a functional definition of the national economic security implications of [FDI] . . . ."[123]

Ultimately, the concern about an "all the above" definition of national security is that it "lead[s] to confusion, waste, [and] distractions, . . . as the U.S. government is asked to do things that are either beyond its capacity or, worse, tangential to the real mission of protecting the country from harm."[124] The overbreadth of CFIUS review resulting from an undefined framework for national security has resulted in many of CFIUS's investigations being problematic for or irrelevant to furthering an overall goal of national security. Moreover, it has led to tremendous restrictions not only on FDI into the U.S. markets, but also on many companies, particularly in the data industry.

IV. DATA PRIVACY IN THE CONTEXT OF NATIONAL SECURITY

How does data privacy fit in with the said notion of national security? Congress and CFIUS seem to think that a necessary consequence of efficiency in ensuring national security is to enforce an

---

121 Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 73 Fed. Reg. 70702, 70705 (Nov. 21, 2008) (describing CFIUS's rejection of comments that national security be defined in favor of a case-by-case review); *see also* Christopher M. Weimar, Note, *Foreign Direct Investment and National Security Post-FINSA 2007*, 87 TEX. L. REV. 663, 674 (2009) ("Like the term 'national security,' many of the above-mentioned factors are intentionally left open to interpretation by the Executive.").

122 *See* discussion *infra* Section VI.A comparing the recent CFIUS transactions.

123 JACKSON, CRS RL33388, *supra* note 20, at 39.

124 Kim R. Holmes, *What is National Security?*, HERITAGE FOUND. (Oct. 7, 2014), https://www.heritage.org/military-strength-topical-essays/2015-essays/what-national-security [https://perma.cc/2DGA-N9TK].

overinclusive, all-encompassing infrastructure of CFIUS review over data privacy.[125] Of late, U.S. officials have begun to treat data privacy as a national security concern because of "concerns about the technology policies of rival powers, most notably the Chinese party-state."[126] Robert Williams, executive director of the Paul Tsai China Center at Yale Law School, argues that it is "entirely legitimate to be concerned that Chinese companies might become vehicles that exploit the relatively open U.S. data environment for purposes that threaten national security, commercial interests, or political values . . . ."[127] However, Scott Charney, corporate vice president of trustworthy computing at Microsoft, has argued that we cannot achieve cyber security by "trying to single out firms of a particular nationality or firms with production in a particular country."[128] Likewise, data privacy cannot be fully achieved by targeting any one single country, particularly a country such as China, which is not even one of the top five countries with the largest amounts of FDI in the United States.[129]

Consequently, suggestions have been made for a privacy protection legal framework that takes national security concerns into account.[130] Williams contends that a national federal privacy statute with clear standards for collection, processing, and sharing of personal data would help avoid discrepancies and inefficiencies, reduce companies' compliance costs, and remove the need for divestment orders or one-

---

125 Jaclyn Jaeger, *Data Privacy vs. National Security: Moving the Conversation Forward*, COMPLIANCE WEEK (Aug. 14, 2019, 3:00 PM), https://www.complianceweek.com/opinion/data-privacy-vs-national-security-moving-the-conversation-forward/27568.article [https://perma.cc/63DK-9H6Q] ("Rather than having data privacy compliance and national security in opposition, with one coming at the expense of the other, it's time to move the needle forward and focus the conversation, instead, on where there are opportunities to collaborate."); Carrie Cordero, *The National Security Imperative of Protecting User Data*, CTR. FOR NEW AM. SEC. (Apr. 24, 2019), https://www.cnas.org/publications/commentary/the-national-security-imperative-of-protecting-user-data [https://perma.cc/T3MC-E2LJ] ("Companies cannot be expected to self-regulate to a sufficient degree that protects Americans from a hostile nation-state intelligence activity.").

126 Robert D. Williams, *To Enhance Data Privacy, Federal Privacy Legislation is Just a Start*, BROOKINGS INST. (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ [https://perma.cc/MGP3-3G95].

127 *Id.*

128 MORAN & OLDENSKI, supra note 11, at 67.

129 News Release, Bureau of Econ. Analysis, *supra* note 10 (discussing the five countries who account for most of the FDI in the United States: Japan, Canada, the United Kingdom, the Netherlands, and Germany).

130 Williams, *supra* note 126.

off presidential authorities for transaction bans.[131] Williams also argues that what a federal data protection scheme fails to address can be provided for by an "effective, tailored mechanism" run by CFIUS "to safeguard national security while restoring confidence in the United States' open economic system."[132]

However, while thought-provoking, the United States still does not have any central federal privacy law, nor any close analog in its domestic privacy law to FIRRMA's sensitive data provision.[133] If the data privacy situation is as dangerous as CFIUS makes it out to be, Congress should implement its own laws contemplating these dangers within the domestic privacy context without merely relying on CFIUS, a national security regulatory scheme, to take on a data privacy framework as well.[134] Allowing data privacy to be contained under the expansive umbrella of CFIUS ultimately provides a legal structure which lacks the specificity necessary to fully address all data privacy concerns and issues.[135] Further, though CFIUS is often used to protect U.S. information from foreign actors, the government has many other available tools such as establishing targeted executive orders for specific Chinese actors, conducting broader reviews of foreign technology in U.S. information and communications technology, and limiting the U.S. government's use of technology from certain foreign providers.[136]

---

131 *Id.*

132 *Id.*

133 Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws/ [https://perma.cc/8XRS-PDJ7].

134 A counterargument to this statement may be that while citizens can trust their own domestic governments to protect their sensitive personal data, this information cannot be entrusted in the hands of foreign governments. However, if the regulations claim such information is so highly sensitive and personal to individuals, there should be a legal regime to enforce targeted protections over such data regardless of who will be the violators of such breaches.

135 Note that in 2002, Scott Charney testified before the House of Representatives and explained how the government is "composed of different organizations to deal with crime, espionage, and war" and they must coordinate a system in which one government agency will lead the response to cyber-attacks and decide which legal authorities will follow. *Speech Transcript – Scott Charney, Testimony Before the U.S. House of Representatives*, MICROSOFT (July 24, 2002) https://news.microsoft.com/speeches/speech-transcript-scott-charney-testimony-before-the-u-s-house-of-representatives/ [https://perma.cc/BKW6-BH8H].

136 Michael E. Leiter & Katie Clarke, *CFIUS' First Full Year Under FIRRMA*, SKADDEN (Jan. 21, 2020), https://www.skadden.com/insights/publications/2020/01/2020-insights/cfius-first-full-year-under-firrma [https://perma.cc/8QNV-VE6S].

Experts have opined on the intrinsic problems within individual companies that attempt to allow both security and privacy professionals to jointly handle data protection, since there is an inherent tension between viewing data as an asset to protect or viewing it as a resource to collect and use to achieve business goals.[137] Likewise, the motivations of a national security statutory regime are not perfectly aligned with that of data privacy and protection. Therefore, since FIRRMA's sensitive data factor acts as the de facto privacy protection legal framework against foreign data access, not only does it fail to protect data privacy, but CFIUS also exceeds its mandate and in effect blocks off the U.S. economy from benefitting from FDI.

The regulations have caused the explosion of many unnecessary CFIUS reviews over harmless transactions involving data related industries and tech companies, where CFIUS could have been focusing resources on actual national security concerns.[138] Further, the opacity of the process prohibits investors from being on notice for what will trigger CFIUS's scrutiny since prior CFIUS reviews "have ranged from the obvious (the acquisition of a US business with federal defense contracts) to the seemingly benign (investments in offshore windfarm projects)."[139] Some commentators have even stated that to understand how CFIUS thinks about personal data requires some imagination, to truly think about what a hostile foreign intelligence service or terrorist organization would be able to do with certain data.[140] As data becomes a greater commodity in the market, the perpetuation of an overly broad concept of national security under the CFIUS regime will ultimately inhibit the globalization of U.S. companies in the data sphere.

---

137 *Microsoft Research Reveals New Trends in Cybercrime*, MICROSOFT (Oct. 23, 2007), https://news.microsoft.com/2007/10/23/microsoft-research-reveals-new-trends-in-cybercrime/ [https://perma.cc/L6ZD-LPWT].

138 Joshua C. Zive, *Unreasonable Delays: CFIUS Reviews of Energy Transactions*, 3 HARV. BUS. L. REV. ONLINE 169 (Apr. 18, 2013), https://www.hblr.org/2013/04/unreasonable-delays-cfius-reviews-of-energy-transactions/ [https://perma.cc/HH3X-25B6].

139 Christopher Kimball & Kevin King, *CFIUS Overview, Committee on Foreign Investment in the United States*, COOLEY, https://www.cooley.com/services/practice/export-controls-economic-sanctions/cfius-overview [https://perma.cc/UHS7-S34J] (last visited Jan. 15, 2022).

140 Hanke & Reeves, *supra* note 17.

V. STATUTORY INTERPRETATION OF THE "SENSITIVE DATA" PROVISION

As a matter of statutory interpretation, the "sensitive personal data" factor should be construed narrowly to cover some, but not all, privacy issues because only some privacy issues implicate national security and, as defined, the regulations are stifling FDI in the U.S. economy.

FIRRMA uses the term "sensitive personal data," and the regulations create a structure upon which CFIUS review for such transactions could be predicated. The regulations chose to define sensitive personal data as either identifiable or genetic data, and further subdivided identifiable data to consist of ten categories.[141] However, a transaction merely falling into one of these categories does not necessarily mean it is sufficiently "sensitive" from a national security perspective.

To this point, the "Sense of Congress" factor which the President and Congress may consider with regard to the use of data is extremely expansive: "[t]he extent to which a transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of U.S. citizens to access by a foreign government or person that may exploit that information to threaten national security."[142] In fact, scholars have pointed to this imprecise factor as the basis for allowing CFIUS review over the TikTok transaction.[143]

Moreover, some of the categories within the regulations are also too broad and thereby overinclusive, generating many unnecessary CFIUS reviews. Specifically, the category of "non-public electronic communications," which includes "email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications," is far too expansive.[144] Of late, CFIUS has relied heavily on this questionable category in its reviews, which has spawned too many futile CFIUS reviews over data privacy transactions, such as TikTok and WeChat.[145]

---

141 31 C.F.R. § 800.241(a)(1)(ii)(A)–(J) (2021).

142 JACKSON, CRS RL33388, *supra* note 20, at 13.

143 William Alan Reinsch, *TikTok Is Running Out of Time: Understanding the CFIUS Decision and Its Implications*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 2, 2020), https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications [https://perma.cc/8KD4-UBCY].

144 31 C.F.R. § 800.241(a)(1)(ii)(E) (2021).

145 Reinsch, *supra* note 143.

This category of sensitive personal data, provided it is referring to civilian communications, at first blush does not seem to implicate national security issues requiring protection of "fundamental values" or "core interests."[146] While companies such as TikTok collect large datasets of such communications, they are most often anonymized in such quantities, and thereby should not pose a security issue.[147] However, scholars have argued that large quantities of personal data, even if anonymized, can be hacked using malware or ransomware, and proprietary algorithms stolen for "misuse and manipulation."[148] Further, the definition of "identifiable data" under the Treasury regulations covers anonymized aggregated data if a foreign investor would be able to de-anonymize the data.[149] While this is certainly true, such concerns would be better left for a cybersecurity or data privacy regime, not to be reviewed by CFIUS and consequently constrain FDI and the U.S. economy.

While it may be conceivable that the regulations were intentionally left overly broad to include more data-related transactions, the regulations have not retained such broad authority in all the categories. In fact, regarding financial information, rather than broadly defining *all* financial data as sensitive, the regulations specify that financial data which is sensitive includes "data that could be used to analyze or determine an individual's financial distress or hardship,"[150] which helps narrow it appropriately. Not only do the regulations limit the sensitivity of financial data to that which is related to financial distress or hardship, but more specifically, the regulations were only concerned with whatever data was used to analyze such conditions, not even the fact of the condition itself. On the other hand, the non-public electronic communications definition has been left overbroad and does not have an equivalent constraint.

Ultimately, the relative breadth of the Sense of Congress factors and so-called non-public electronic communications subcategory opens a forum for a vast array of concerns in the national security

146 JORDAN ET AL., *supra* note 114.

147 Susan Ariel Aaronson, *Why Personal Data Is a National Security Issue*, BARRON'S (Aug. 12, 2020, 11:00 AM), https://www.barrons.com/articles/why-personal-data-is-a-national-security-issue-51597244422 [https://perma.cc/JMP5-7XGQ].

148 *Id.*

149 Mortlock, Goheer, Ed-Gamal, *supra,* note 104.

150 31 C.F.E. § 800.241(a)(1)(ii)(A).

sphere, as well as Constitutional concerns regarding the First Amendment.[151]

A. Comparing Recent Data Transactions Blocked by CFIUS as a Matter of Statutory Interpretation

Commenters have likened the current CFIUS strategy to "company-whack-a-mole" arguing that "[c]ase-by-case attacks on particularly powerful Chinese-controlled companies can't adequately address the underlying trends and concerns."[152] Nevertheless, privacy concerns are not baseless due to "the fragmentary nature of data privacy laws, [as] it can be extremely difficult to ensure the security of your data . . . ."[153] Therefore, it is critical to analyze a few of the many CFIUS reviews over data related transactions to assess which did implicate national security concerns, as opposed to those that were unnecessary or irrelevant.

Though CFIUS is notorious for not providing reasoning for blocking transactions, in January of 2018, MoneyGram and Ant Financial announced the termination of a planned acquisition of MoneyGram by Ant Financial.[154] The transaction did not pass muster under CFIUS review, with some "sources stating that the security of Americans' financial data was [the] major concern."[155] The FIRRMA regulations later solidified such decisions as being under CFIUS

---

151 Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1151 (2005); Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020, 2:53 PM), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html [https://perma.cc/53LN-SHXF]; *First Amendment and Censorship*, AM. LIBR. ASS'N, http://www.ala.org/advocacy/intfreedom/censorship [https://perma.cc/R44W-RH2Y] (Oct. 2021).

152 Jennifer Daskal & Samm Sacks, *The Furor Over TikTok Is About Something Much Bigger*, SLATE (Nov. 8, 2019), https://slate.com/technology/2019/11/tiktok-bytedance-china-geopolitical-threat.html [https://perma.cc/M567-DTMS].

153 Jeff Petters, *Data Privacy Guide: Definitions, Explanations and Legislation*, VARONIS (Sept. 28, 2020), https://www.varonis.com/blog/data-privacy/ [https://perma.cc/P2TD-BAWQ].

154 Greg Roumeliotis, *U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns*, REUTERS (Jan. 2, 2018, 4:36 PM), https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7 [https://perma.cc/CG8H-7P6E].

155 Robert Kim, *Analysis: CFIUS Scrutiny Forces Chinese Sale of Grindr*, BLOOMBERG L. (Apr. 16, 2019, 3:48 PM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-cfius-scrutiny-forces-chinese-sale-of-grindr [https://perma.cc/73KG-79JC].

jurisdiction by incorporating a subcategory of "sensitive personal data"—"data that could be used to analyze or determine an individual's financial distress or hardship."[156] MoneyGram, as a money services business that loans money to nearly 100 million individuals, has a large collection of personal data which can be used to determine financial distress or hardship, and therefore, this transaction was certainly within CFIUS's reach.[157]

CFIUS has also exhibited concerns with data maintained by dating services and related mobile applications. In 2019, CFIUS pressured Beijing-based Kunlun Tech Co. to divest from Grindr, an LGBTQ+ dating app whose database contains personal information such as users' locations, messages, sexual orientations, and HIV statuses.[158] Here, commentators noted that "Grindr's collection of personal data makes privacy and personal security into significant concerns even in the absence of any national security issues."[159] As such, scholars seem to argue that protection of some types of sensitive data, such as sexual orientation, should be ushered into a national security system of enforcement even if they do not pose actual security concerns. The divestment of Grindr was a "[r]are, high-profile example of CFIUS undoing an acquisition that has already been completed."[160] Thus, CFIUS managed to reach its apex of control with Grindr, undoing an already completed transaction, for data which did not necessarily pose a security issue, even if the data was highly sensitive.

Though "the reasoning of CFIUS on Grindr's case may not be clearly ascertainable," it fits a very clear trend to block any transactions with a concern for the security of U.S. data.[161] Grindr represents

---

156 31 C.F.R. § 800.241(a)(1)(ii)(A) (2021).

157 *See MoneyGram International Reports Second Quarter 2021 Results*, MONEYGRAM (July 30, 2021), https://ir.moneygram.com/node/22236/pdf [https://perma.cc/2K8Z-9PMX].

158 Kim, *supra* note 155.

159 *Id.*

160 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/chinas-kunlun-tech-agrees-to-u-s-demand-to-sell-grindr-gay-dating-app-idUSKCN1SJ28N [https://perma.cc/9XJG-4UJU].

161 Kim, *supra* note 155; *see also* Danzman & Gertz, *supra* note 24 ("But the notion that a dating app could threaten national security is not as ludicrous as it seems. Like other social networking companies, Grindr keeps a lot of social data on its customers, including U.S. officials and government contractors who could be blackmailed or compromised. Moreover, since Grindr uses geolocation, it can track its users' movements. Although it is impossible to know precisely why CFIUS intervened in this case — the agency is secretive and never discloses the specific

the idea that CFIUS is open to an expansive view of possible threats to U.S. national security, particularly in the context of intimate personal relationships. More specifically, personal data found on Grindr can be "a tempting target for foreign intelligence" to use to blackmail or embarrass individuals and government officials.[162]

Under FIRRMA, the information collected by Grindr falls within the purview of what the regulations define as sensitive personal data. Interestingly, information such as sexual orientation would not necessarily be considered sensitive personal data under any of the Treasury Department regulations' categories. Further, under the categorization of genetic data, HIV status would not qualify as genetic information, since "genetic tests" do not include "an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved."[163] However, the data contained on the application, such as "non-public electronic communications" and "geolocation data," would still be considered sensitive under the regulations as identifiable data.[164] Such data is identifiable since it "can be used to distinguish or trace an individual's identity . . . through the use of [a] personal identifier."[165] However, it remains questionable whether the undoing of such a transaction should have been within CFIUS's power altogether.

Likewise, in the medical data realm, PatientsLikeMe, an American data company that connects patients to others with like health conditions, was forced by CFIUS to find a U.S. buyer and divest itself of a $100 million stake by Chinese genetic research firm iCarbonX.[166] Though this transaction preceded the final regulations of FIRRMA, the data would be considered within the regulations' subcategory of sensitive personal data as "[d]ata relating to physical, mental, or psychological health condition of an individual."[167] This transaction

justifications for its decisions — reporting suggests these data privacy issues were an important factor.").

162 Kim, *supra* note 155.

163 42 U.S.C. § 300gg-91(d)(17)(A), (d)(17)(B)(ii).

164 31 C.F.R. § 800.241(a)(1)(ii)(E), (a)(1)(ii)(F) (2021).

165 31 C.F.R. § 800.226; *see also* 42 U.S.C. § 300gg-91(d)(17)(A), (d)(17)(B)(ii); 31 C.F.R. § 800.238.

166 Muoio, *supra* note 25; *see also* Laura Lovett & Dave Muoio, *UnitedHealth Group Acquires PatientsLikeMe*, MOBIHEALTHNEWS (June 24, 2019, 3:39 PM), https://www.mobihealthnews.com/content/unitedhealth-group-acquires-patientslikeme [https://perma.cc/M4ZM-H2RV].

167 31 C.F.R. § 800.241(a)(1)(ii)(D).

should have been beyond the scope of CFIUS jurisdiction because PatientsLikeMe reportedly had data on no more than 830,000 people with 2,800 health conditions, which does not hit the 1 million individual threshold.[168] Additionally, this information does not constitute genetic information, since "genetic test" does not include "an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved."[169] Thus, the blocking of PatientsLikeMe demonstrates a CFIUS review which was unnecessary and burdensome to an American-owned company with merely a foreign-held stake.

CFIUS then started to review and block transactions in the realm of social media. In March of 2019, upon CFIUS's decision to block the transaction, the Trump administration ordered Beijing Shiji Information Technology to divest all interests in StayNTouch.[170] Though CFIUS provided no reasons, perhaps StayNTouch's use of "travel-related personal information" and "software tools [that] leverage ID scanning and facial recognition technology . . ." was considered identifiable data.[171] CFIUS also decided to retroactively investigate ByteDance's acquisition of Music.ly, for which Music.ly did not even submit a review for national security concerns.[172]

---

168 *Empowering Patients Through Community*, PATIENTSLIKEME, https://www.patientslikeme.com/about [https://perma.cc/YJ93-6LRJ] (last visited Mar. 4, 2022). Note that although the Treasury Department Regulations state that the data threshold is one million individuals, the regulations further delineate that it is accounted over a twelve-month period, and the types of data held can be aggregated or include the company's data retention policy to allow CFIUS to consider the threshold met. *See* 31 C.F.R. § 800.241(a)(1)(i)(B). However, since in its own biography PatientsLikeMe indicates that they have treated over 850,000 people and do not list a higher number, it is unlikely that they ever had one million individual users' data. While the Treasury Department regulations provide examples for how data may be aggregated, it remains unclear how CFIUS did so regarding this transaction. *See* 31 C.F.R. § 800.241(c).

169 42 U.S.C. § 300gg-91(d)(17)(B)(ii).

170 Jeanne Whalen, *Trump Orders Chinese Company to Divest Ownership of U.S. Firm, Citing National Security Concerns*, WASH. POST (Mar. 6, 2020), https://www.washingtonpost.com/business/2020/03/06/trump-orders-chinese-company-divest-ownership-us-firm-citing-national-security-concerns/ [https://perma.cc/L8VP-TBNK].

171 *President Trump Orders Divestiture of StayNTouch, Inc. by Shiji Group of China*, COVINGTON (Mar. 9, 2020), https://www.cov.com/en/news-and-insights/insights/2020/03/president-trump-orders-divestiture-of-stayntouch-inc-by-shiji-group-of-china [https://perma.cc/4JJD-LPVM].

172 Reinsch, *supra* note 143.

The essential national security fears presented by TikTok include: (1) China's potential ability to use and exploit U.S. personal information collected by the platform, and (2) Chinese influence operations. The concerns are legitimate. TikTok as a social network "is collecting a lot of data,"[173] including information such as users' contact details, content users create, users' locations, information from third-party social network providers, technical and behavioral information about users' use of the platform, information contained in the messages users send through the TikTok platform, and information from users' phonebooks.[174]

Under the Cybersecurity Law of 2017, the Chinese government can request information from any company operating in China.[175] Chinese actors, however, have claimed that there is leeway to negotiate the scope of such requests.[176] In fact, according to Chinese President Xi Jinping, many Chinese companies routinely push back against data requests from the government, and the government does not necessarily have real time access to all companies' data. [177] Whether or not the veracity of such claims has a basis, almost all the data on TikTok is comprised of young adults communicating, acting, dancing, singing, cooking, and expressing themselves creatively, and, therefore, will likely be of limited to nil value to the Chinese government.[178] Further, common uses for data collection are for the purposes of advancing business goals or for espionage. The entertainment-based platform may be immensely helpful for the former as e-commerce businesses

---

173 *Senate Subcommittee Hearing on Data Breaches*, C-SPAN, at 35:54 – 36:06 (Nov. 5, 2019), https://www.c-span.org/video/?466062-1/senate-subcommittee-hearing-data-breaches [https://perma.cc/KCQ9-2UNH]. (statement of Sen. Josh Hawley, Member, S. Judiciary Subcomm. on Crime & Terrorism).

174 *Id.* at 36:11–36:32.

175 Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, DIPLOMAT (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ [https://perma.cc/P66Z-3CYQ].

176 Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, LAWFARE, (Apr. 2, 2020, 8:00 AM), https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement [https://perma.cc/YPJ8-LWAU] (noting that some examples include Chinese ride-sharing app, Didi, refusing to give data to investigate murder of passengers, and Tencent and Alibaba refusing to share transaction data with the Bank of the Republic of China); *see* Yuan Yang & Nian Liu, *Alibaba and Tencent Refuse to Hand Loans Data to Beijing*, FIN. TIMES (Sept. 18, 2019), https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17 [https://perma.cc/6K4X-5NVH].

177 *Id.*

178 Reinsch, *supra* note 143 ("Regardless, given that the platform is predominately used by young adults, the majority of TikTok users' data is likely to be of limited value to the Chinese government.").

target Generation Z audiences on the application, but TikTok is likely unhelpful to aid China in spying or finding a back door into the United States.[179]

In an interview with David Rubinstein, TikTok's CEO Shou Zi Chew explained how TikTok took necessary steps to separate from China, including barring the application's use in China, ceasing operations with Hong Kong, and storing data in Virginia and Singapore.[180] Further, Chew discussed how TikTok's algorithms measuring user likes, comments, and activity are solely used "to digest user behavior" to tailor each user's experience on the application to their unique interests.[181] Much of the TikTok data collected, such as user activity, and "For You" pages would not be considered sensitive even under the regulations' categories. However, the application does collect enormous amounts of "non-public electronic communications," "geolocation data," and perhaps even some information relating to the "physical, mental, or psychological health condition of an individual."[182] While this information may be sensitive, concerns over TikTok's data does not pose concerns such that CFIUS should have been at all involved. Rather, such issues belong in a cybersecurity or data privacy legal regime.

Another concern is the possibility of Chinese influence operations through propaganda or censorship. Since TikTok is not available for download in China, this seems unlikely. Further, on a pedantic note, such operations, given the platform, are unlikely to be useful amongst American young adults. However, there may be First Amendment concerns regarding policing or censoring of content based on sensitivities related to China, which would be unconstitutional.[183]

More recently, Judge Rudolph Contreras "blocked enforcement of the U.S. investment ban on Xiaomi Corp., calling the decision to

---

179 *Microsoft Research Reveals New Trends in Cybercrime*, *supra* note 137.

180 *See The David Rubinstein Show: TikTok CEO Shouzi Chew*, BLOOMBERG (Mar. 3, 2022, 5:18 AM), https://www.bloomberg.com/news/videos/2022-03-03/the-david-rubenstein-show-tiktok-ceo-shouzi-chew-video [https://perma.cc/55P8-KBK9].

181 *Id.* Note that the TikTok application has a feature known as the "For You" page which contains videos and multimedia geared to each user's specific interests based on their daily activity on the application and how long they spent watching certain content. *What Is the 'For You' Feed?*, TIKTOK, https://www.tiktok.com/creators/creator-portal/en-us/tiktok-creation-essentials/whats-the-for-you-page-and-how-do-i-get-there/ [https://perma.cc/QG2W-2GZE] (last visited Mar. 4, 2022).

182 31 C.F.R. § 800.241(a)(1)(ii)(D)–(F) (2021).

183 *Id.*

blacklist the Chinese technology giant 'deeply flawed.'"[184] Likewise, TikTok's investment ban was stalled by the D.C. Circuit, seemingly following a trend in the U.S. courts to limit CFIUS's power with regard to data-related transactions.[185] Given all of the above reasons, the type of data collected and maintained by TikTok should have been outside of the purview of CFIUS review.[186]

VI. POLICY BEHIND CFIUS DATA PRIVACY PROTECTIONS

As a matter of policy, Congress should not have added the "sensitive personal data" factor in the first place because it captures sectors that are fundamentally different from the other types of sectors that fall within CFIUS's national security mandate, and data privacy does not fully belong within the national security sphere.[187] Most data privacy concerns cannot be addressed by a CFIUS regime which only cares about data in relation to national security, and as such, data

184 Dan Strumpf, *Xiaomi Wins Court Ruling Halting U.S. Investment Ban*, WALL ST. J. (Mar. 12, 2021, 11:31 PM), https://www.wsj.com/articles/xiaomi-wins-court-ruling-halting-u-s-investment-ban-11615604756?mod=hp [https://perma.cc/3CF2-DM4B].

185 David Shepardson & Steve Holland, *U.S. Asks Courts to Put TikTok Appeals on Hold Pending Biden Team Review*, REUTERS (Feb. 10, 2021), https://www.reuters.com/article/us-usa-tiktok-bytedance-biden/u-s-asks-courts-to-put-tiktok-appeals-on-hold-pending-biden-team-review-idUSKBN2AA1GR [https://perma.cc/L4H3-766J] ("Three federal judges in separate rulings blocked Commerce orders on TikTok and for Chinese-owned WeChat."); Russell Brandom, *The TikTok-Oracle Deal Is on Life Support Under Biden*, The Verge (Feb. 10, 2021), https://www.theverge.com/2021/2/10/22276090/tiktok-oracle-deal-biden-trump-ban-china-bytedance-white-house [https://perma.cc/833G-V6MN] (stating that the TikTok-Oracle "deal was stalled by a string of successful court challenges to the August 6th order").

186 31 C.F.R. § 800.241 (2021); *see also* Martin Chorzempa, *The TikTok Deal Is a Defining Moment for CFIUS*, BARRON'S (Sept. 17, 2020, 9:54 AM), https://www.barrons.com/articles/the-tiktok-deal-is-a-defining-moment-for-cfius-51600350898 [https://perma.cc/93VK-3AB8]; Taylor Walshe & Shining Tan, *TikTok on the Clock: A Summary of CFIUS's Investigation into ByteDance*, CTR. FOR STRATEGIC & INT'L STUD. (May 13, 2020), https://www.csis.org/blogs/trustee-china-hand/TikTok-clock-summary-cfiuss-investigation-bytedance [https://perma.cc/894M-U9F2]; Robert Chesney, *The Latest TikTok Order: Comparing the New CFIUS Order to the Prior IEEPA Order*, LAWFARE (Aug. 18, 2020, 3:53 PM), https://www.lawfareblog.com/latest-tiktok-order-comparing-new-cfius-order-prior-ieepa-order [https://perma.cc/S4VS-5YUR].

187 Amy Deen Westbrook, *Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions*, 102 MARQ. L. REV. 643, 673 (2019); *see also* MORAN & OLDENSKI, *supra* note 11, at 70 (analyzing how the recent blocked data transactions do not fall within the Peterson categories of CFIUS threats).

privacy should not be completely engulfed by CFIUS's overly broad mandate.

First, "FIRRMA provided no definition whatsoever for 'sensitive personal data,'" which is in "stark contrast to the new law's treatment of the two other areas where it expanded CFIUS's jurisdiction over minority-position investments. FIRRMA laid out at least a basic definition of 'critical infrastructure,' as well as a highly detailed definition of 'critical technologies.'"[188] This seems to indicate that while legislators were keen to include data as a national security problem under CFIUS review, they have not yet figured out how to do so appropriately. Second, the other relevant sectors over which CFIUS reviews FDI all directly impact national security, while data privacy only indirectly affects national security.[189]

Third, though the CFIUS mandate makes it seem as though it is the only line of defense for protecting foreign-owned data communications, it is not. The United States contains three regulatory vehicles by which to control foreign ownership in the communications sector: the Department of the Treasury ("DOT"), the Federal Communications Commission ("FCC"), and the Department of Justice ("DOJ").[190] The FCC deals with the transfer of licenses and can waive the prohibition against transfer to a corporation with greater than twenty-five percent foreign government ownership if in the public's interest, while the DOJ can review foreign acquisitions for antitrust violations.[191] Lastly, CFIUS, belonging to the DOT, has a review process by which it can block or evaluate foreign transactions, even of non-controlling interests or merely access rights for data-privacy related transactions under the sensitive personal data factor.[192]

A CFIUS mandate, especially one that is vague and overly broad, simply cannot account for all the data privacy issues that can arise in the absence of a domestic or national federal privacy statute, or for all the issues that fall under the DOJ's or the FCC's jurisdiction. Therefore, data privacy does not merely belong nestled amongst the other national security problems in the CFIUS mandate, but rather deserves its own space within DOJ and FCC administration, and perhaps its

188 Hanke & Reeves, s*upra* note 17.

189 *See* James A. Lewis, *New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception*, 57 FED. COMMC'NS L.J. 457, 457 (2005) (explaining that communications interception poses an indirect, but real challenge for critical infrastructure).

190 *Id.* at 463.

191 *Id.*

192 50 U.S.C. § 4565.

own governing rules."In a world where data privacy, digital trade, and national security are increasingly intertwined, the data governance agenda . . . cannot stop" with an all-powerful CFIUS mandate.[193]

A. Comparing Recent Data Transactions Blocked by CFIUS as a Matter of Policy

According to the Peterson Institute for International Economics, there is a method to the CFIUS madness, where "perceived threats to national security from foreign acquisition of a US company fall into three distinct categories."[194] A national security threat includes proposed acquisitions that would: (1) make the "United States dependent on a foreign-controlled supplier for goods or services *crucial* to the functioning of the US economy," with crucial being defined as having a "large negative effect if the economy had to do without the goods and services in question";[195] (2) "allow transfer of technology or other expertise to a foreign-controlled entity that the entity or its government could deploy in a manner harmful to US national interests";[196] or (3) "allow insertion of some capability for infiltration, surveillance, or sabotage—through a human or non-human agent—into the provision of goods or services crucial to the functioning of the US economy," such as the defense industrial base.[197] Despite this specific infrastructure, the article states that CFIUS "has not . . . kept up with the understanding of what constitutes a potential threat to national security or appreciated the relatively rare circumstances in which such a threat might be credible."[198]

Examining the cases discussed above through the lens of the threats posed by transactions under CFIUS review highlights how,

---

193 Williams, *supra* note 126.

194 MORAN & OLDENSKI, *supra* note 11, at 55; *see also id.* at 55–72.

195 *Id.* at 55–58 (emphasis added) (describing that part of the evaluation of Threat I can be whether there is a "credible likelihood that the good or service can be withheld–or that the suppliers or their home governments, could place conditions on providing the good or service").

196 *See id.* at 55. Under this category, the questions which arise include: How broadly available is the managerial or production expertise available? Would this acquisition make a difference for the new home government?

197 *Id.*

198 *Id.* at 56, 60 (looks to whether the foreign acquisition offer the new owner's government an opportunity to penetrate, or "a platform for clandestine observation or disruption"). There lies an opportunity for mitigation within this category, e.g., creating vetting procedures or inputting U.S. operations over aspects of the company, such as was attempted in the 2005 Dubai Ports case, which were ultimately rejected. *Id.* at 60–61.

policy-wise, data privacy does not quite fit into the national security scheme. The would-be acquisition of MoneyGram by Ant Financial would not make the United States dependent on a foreign-controlled supplier or provide technology or expertise to a foreign government so Threats 1 and 2, above, would not apply. Further, even if the acquisition of MoneyGram would allow the insertion of some capability for surveillance, it would not unveil anything crucial to the functioning of the U.S. economy, and thus would not fall under Threat 3 either.

Similarly, Threats 1 and 2 would not apply to the cases of both Grindr and PatientsLikeMe. The types of information Grindr and PatientsLikeMe gather, such as medical information, location, sexual orientation, and HIV status, may be sensitive, but it is not ultimately crucial to the functioning of the American economy. Further, given the low number of 830,000 users of PatientsLikeMe, it had not reached the critical threshold amount reviewable by CFIUS. Lastly, the TikTok transaction—wherein TikTok already has separations in place and stores data in countries other than China for national security concerns—does not fit into any of the above threats, and arguably does not allow for infiltration or espionage, given all its current constraints.

When Huawei was blocked from AT&T and Sprint Nextel contracts for national security concerns, the company set forth an intensive security model, which the Peterson Institute indicated "extend[ed] far beyond concerns about foreign acquisitions of local companies."[199] Similar to the cyber-security sector, under the current CFIUS regime, the data-privacy sector is becoming highly regulated and constrained. Data-collection companies will be forced to input expensive, unnecessary infrastructure to avoid CFIUS review when transacting with foreigners who want to enter U.S. markets. The data-privacy sector is simply too large and broad to be wholly encapsulated as a national security concern. Currently, any mildly ambitious company with more than one million users who attempts to transact globally will run into issues under the CFIUS regulations regarding personal data.[200]

From a policy perspective, while there is certainly a place for data privacy under the umbrella of national security, due to the regulations' overly expansive categories, CFIUS review has become far too all-encompassing. The definition for non-public communications should certainly be cabined or limited in a meaningful way.

---

199 MORAN & OLDENSKI, *supra* note 11, at 67.

200 31 C.F.R. § 800.241(a)(1)(i)(A)–(C) (2021).

VII. CONCLUSION

Where is TikTok now? Since the initial August 2020 executive order, a long, contentious legal battle has followed in the United States courts between former President Trump and TikTok creators Douglas Marland, Cosette Rinab, and Alec Chambers, as the creators contest the legality, under the First and Fifth Amendments, of forcing TikTok to divest all its assets of at least 100 million American users to an American-owned company, or face a download ban creators.[201] The Department of Commerce later pronounced that it would comply with a second injunction granted by Judge Wendy Beetlestone in the creators' case, and the DOJ has since filed an appeal.[202]

Additionally, His executive order's significance is nil in the case of TikTok, since TikTok is still subject to the divestment order under CFIUS. However, for now, the TikTok-Oracle deal had been "shelved indefinitely" while President Biden reviews the Trump Administration's China policy.in TikTok's own challenge, Judge Carl Nichols of the U.S. District Court for the District of Columbia granted TikTok's request for an injunction as of the initial divestment deadline.[203] President Joe Biden has stated that it is a "matter of genuine concern that TikTok, a Chinese operation, has access to over 100 million young people particularly in the United States of America."[204] On June 9, 2021, however, President Biden issued an executive order revoking the sanctions.[205] His executive order's significance is nil in the case of TikTok, since TikTok is still subject to the divestment order under CFIUS. However, for now, the TikTok-Oracle deal had been "shelved

---

201 Andrew Hutchinson, *TikTok Stars Win Injunction Against White House Executive Order, Keeping the App Running the US*, SOC. MEDIA TODAY (Oct. 30, 2020), https://www.socialmediatoday.com/news/tiktok-stars-win-injunction-against-white-house-executive-order-keeping-th/588173/ [https://perma.cc/5VC9-CFGD].

202 *See* Reuters, *TikTok Gets Another Reprieve from Order That Would Ban It in U.S.*, N.Y. TIMES (Oct. 30, 2020), https://www.nytimes.com/2020/10/30/business/tiktok-injunction-ban.html [https://perma.cc/VT8L-4CMG].

203 *See* TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 115 (D.D.C. 2020).

204 *Biden Says He Sees TikTok as a 'Matter of Genuine Concern'*, REUTERS (Sept. 18, 2020, 6:57 PM), https://www.reuters.com/article/us-usa-tiktok-ban-biden/biden-says-he-sees-TikTok-as-a-matter-of-genuine-concern-idUSKBN26938G [https://perma.cc/FV38-LXPG].

205 Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019); *see also* 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 [https://perma.cc/HM2Z-VXJP].

indefinitely" while President Biden reviews the Trump Administration's China policy.[206]

TikTok, Grindr, and PatientsLikeMe are paradigmatic examples under the current CFIUS regime which demonstrate how the costs of an overly broad and vague CFIUS mandate are astronomical.[207] For parties making data related deals, it greatly lessens their incentive since "the failure to define national security" within the context of data privacy "increases uncertainty and delays transactions, significantly reducing the deals' value," and moreover, parties would not like to expend time and money structuring a deal which will all be for naught when CFIUS comes and blocks it from going through.[208] Foreign companies are also less likely to attempt to enter U.S. markets. Furthermore, this heightens the Committee's expenses for monitoring and review as well, as in the "absence of clear direction regarding the national security review," there will be many more voluntary, unnecessary notices for CFIUS to wade through.[209] Due to the lack of reasoning given to the public by CFIUS for their decision-making process, U.S. presidents or the Committee may make politically motivated decisions rather than decisions in the interest of national

206 John D. McKinnon & Alex Leary, *TikTok Sale to Oracle, Walmart Is Shelved as Biden Reviews Security*, WALL ST. J. (Feb. 10, 2021, 5:40 PM), https://www.wsj.com/articles/TikTok-sale-to-oracle-walmart-is-shelved-as-biden-reviews-security-11612958401 [https://perma.cc/R7DV-AXRD]. If any data-hosting partnership were to move forward, a question arises about how U.S. user data will be localized and kept in the United States. Some options include local cloud service providers or encrypting data and keeping the encryption keys elsewhere. The arrangement will need to account for such logistics as when or if law enforcement agencies will be able to access such data or where encryption keys will be kept. *See* Williams, *supra* note 126.

207 Tipler, *supra* note 83, at 1224 (noting that there is no accurate measure of these costs, but an analysis of the CFIUS review process, available data, case studies of significant cross-border deals, and other available information demonstrates that these costs are substantial.); *see also* Daniel P. Brooks & Nova J. Daly, *New Bill Would Allow CFIUS to Scrutinize Gifts to Higher Education*, WILEY (Apr. 13, 2021), https://www.wiley.law/alert-New-Bill-Would-Allow-CFIUS-to-Scrutinize-Gifts-to-Higher-Education [https://perma.cc/UJJ3-QJCY] (discussing an overly broad CFIUS mandate).

208 Tipler, *supra* note 83, at 1224–25 (noting that the entire CFIUS process could take ninety days with the thirty-day review, forty-five-day investigation, and fifteen-day presidential decision process); *see also* Shearer, *supra* note 64, at 1768 (noting that because "the 'national security' standard is susceptible to various interpretations, foreign investors face many uncertainties when structuring acquisitions involving a company engaged in U.S. interstate commerce") (citation omitted).

209 Tipler, *supra* note 83, at 1225.

security.[210] Lastly, host countries whose companies' transactions get blocked may retaliate or feel hostility toward the United States, resulting in large decreases in FDI, or worse.[211] Beyond the crushing blow that the loss of FDI revenue would cause to the U.S. economy, this may be fatal to the United States in its foreign policy, since the highest investing countries are all allies of the United States.[212]

This Note grapples with whether national security necessarily includes data privacy, and how broadly CFIUS jurisdiction can and should reach within this context. While Congress may not have been perfectly clear on this scheme, we can be certain that the answer is to find "technical solutions to secure data while enabling productive means of sharing it."[213] As Jonathan Hillman, former director of the Reconnecting Asia Project at the Center for Strategic and International Studies, claims that an overly paranoid and defensive reaction to Chinese tech companies risks undermining both the United States' values and its economic competitiveness.[214] "The risk of getting this wrong," Hillman writes, "is not merely that the United States becomes less competitive, but that it also becomes less American."[215]

As for TikTok, despite the unresolved CFIUS divestment order hanging over its head,[216] its U.S. presence has only been expanding,

---

210 ALAN P. LARSON & DAVID M. MARCHICK, FOREIGN INVESTMENT AND NATIONAL SECURITY: GETTING THE BALANCE RIGHT 6 (2006) (stating how state ownership of multinational firms is often benign, but that concerns arise "when the foreign company's decisions become an extension of the government's policy decisions rather than the company's commercial interests").

211 *Id.* at 3.

212 Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(a)(3)(B), 132 Stat. 2174; Masters & McBride, *supra* note 13 (noting that to avoid this, "thirty-four members of the Organization for Economic Cooperation and Development (OECD), as well as twelve nonmember states, have signed a nonbinding commitment to treat foreign-controlled firms on their territories no less favorably than domestic enterprises." The issue is that "[g]overnments under this agreement are . . . provided considerable latitude to exempt sectors of their economies deemed essential to national security," which is problematic, since countries define sensitive sectors in different ways).

213 Williams, *supra* note 126.

214 Jonathan Hillman, *Pretending All Chinese Companies Are Evil Schemers Will Only Hurt the U.S. Economy*, WASH. POST (Nov. 8, 2019), https://www.washingtonpost.com/outlook/pretending-all-chinese-companies-are-evil-schemers-will-only-hurt-the-us-economy/2019/11/08/b0d98798-00dc-11ea-9518-1e76abc088b6_story.html [https://perma.cc/ZL7A-4G2X]; *see also* JONATHAN E. HILLMAN, THE DIGITAL SILK ROAD: CHINA'S QUEST TO WIRE THE WORLD AND WIN THE FUTURE (2021).

215 Hillman, *supra* note 214.

216 J. Clara Chan, *TikTok Isn't "Out of the Woods" With Biden's Executive Order, But Creators Are Prepared This Time*, HOLLYWOOD REP. (June 14, 2021, 10:22

with offices opening in New York, and Los Angeles.[217] It seems that even with CFIUS's best efforts to take control of TikTok, its regulation is better suited in the data privacy world for data privacy professionals or the tech experts to handle. We have yet to see how CFIUS's second round of investigations and regulatory measures will fare. If it is anything like the current ongoing divestment order, TikTok should have nothing to fear.

AM), https://www.hollywoodreporter.com/business/business-news/tiktok-bytedance-biden-executive-order-creators-1234967037/ [https://perma.cc/M4CS-2NW5].

217 *Id.* ("[I]f anything, the company continued to grow despite the uncertainty of its future in the U.S."); Vanessa Pappas, *Growing Our Presence in Los Angeles*, TIKTOK (Jan. 22, 2020), https://newsroom.tiktok.com/en-us/growing-our-presence-in-los-angeles [https://perma.cc/9Y6R-3YHF].