Foreign Investment and National Security Challenges in the Data Age: An Assessment of the Current Regime and Recommendations

IRENE YU[†]

This Note contributes to the growing literature that attempts to grasp the current landscape of international trade and investment norms and policies in the data age. Focusing on the disputes between the United States and China surrounding Chinese investment in American businesses that gather private user data, this Note adds to the argument that new challenges posed by the internet age and the use of private data have transformed current international trade policy and the national security exception regime. The U.S. government in the recent years has demonstrated little self-restraint in employing national security grounds to justify its interference with Chinese investment in American companies possessing significant private user data. There is also arguably a lack of remedies from international organizations like the World Trade Organization (WTO) due to the controversy surrounding the use of the national security exception clause.

The Commission on Foreign Investment in the United States (CFIUS), the central mechanism that the U.S. government relies on to regulate foreign investment on American businesses that possess significant private user data, may hinder cross-border transactions due to its expansive authority, coupled with a lack of transparency and accountability. The United States should provide greater transparency and accountability to CFIUS and consider data-localization law as a solution to facilitate foreign investment in American businesses of special concern.

[†] J.D. Candidate 2023, University of California College of the Law, San Francisco (formerly UC Hastings); Executive Symposium Editor, *Hastings Law Journal*. I am appreciative of comments and support from my advisor, Professor Chimène Keitner, and the editors of the *Hastings Law Journal*.

TABLE OF CONTENTS

INTRODUCTION

Businesses that provide digital services by gathering and utilizing private user data are growing rapidly across the globe. As government regulators struggle to keep up with these growing practices, there are also rising national security concerns regarding the threat of foreign actors' abuse of private data.[1] The security challenges posed by this new development influence the United States' foreign investment policies. Growing literature suggests that as governments worldwide adopt policies to address national security risks posed by emerging issues, these policies are likely to conflict with existing trade and investment rules established under the current liberal economic order framework.[2]

National security and trade policies became a hotly contested issue under former President Trump's Administration. The Trump Administration employed hostile rhetoric against China and attempted to pressure China for more accommodating terms on trade, investment, and foreign exchange issues.[3] The United States has also unwound or restricted Chinese investment in American businesses that have gathered significant private data due to national security concerns.[4] Of specific concern, the Chinese acquisition of TikTok has received wide media coverage.

TikTok is a popular social media app owned by the Chinese company ByteDance that provides an online platform where users can upload and share short videos with the public.[5] Former President Trump determined that Chinese ownership of TikTok posed national security threats, as the company possesses vast swaths of user data and may provide the Chinese government access to American users' personal and proprietary information.[6] Further, former President Trump claimed that the app potentially allows the Chinese government to "track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[7] To address the national security threats posed by TikTok, the Trump Administration proceeded with two parallel tracks of action. The first was using the Executive's authorities under the International Emergency Economic Powers Act (IEEPA) to impede the app's U.S. operations.[8] The second tactic was to compel changes

1. *See infra* Part I.

2. J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1020 (2020).

3. Eric Sayers & Ivan Kanapathy, *America Is Showering China with New Restrictions*, FOREIGN POL'Y (Feb. 15, 2022, 2:45 PM), https://foreignpolicy.com/2022/02/15/us-china-economic-financial-decoupling-controls-restrictions-sanctions/.

4. *See United States Pursues Regulatory Actions Against TikTok and WeChat over Data Security Concerns*, 115 AM. J. INT'L L. 124, 124–25 (2020) [hereinafter *Regulatory Actions Against TikTok*].

5. John Herrman, *How TikTok Is Rewriting the World*, N.Y. TIMES (Mar. 10, 2019), https://www.nytimes.com/2019/03/10/style/what-is-tik-tok.html.

6. Exec. Order No. 13,942, 85 Fed. Reg. 48637, 48637 (Aug. 11, 2020).

7. *Id.*

8. *Regulatory Actions Against TikTok*, *supra* note 4, at 125.

in the ownership of TikTok through the Committee on Foreign Investment in the United States (CFIUS).[9]

Besides TikTok, the Trump Administration also rejected and instructed the unwinding of mergers and acquisitions involving Chinese investment in other American businesses possessing significant private user data.[10] The unprecedented actions against Chinese investment under the Trump Administration deviated from the conventional use of a national security exception under current trade and investment policies, and they are not likely a one-off incident. The Biden Administration has continued this practice and will likely expand such actions.[11]

This Note contributes to the growing literature that attempts to grasp the current landscape of international trade and investment norms and policies in the data age. Focusing on the disputes between the United States and China surrounding Chinese investment in American businesses that gather private user data, this Note adds to the growing argument that new challenges posed by the internet age and the use of private data have transformed current international trade policy and the national security exception regime. While governments have a stake in protecting their national security interests, economic measures taken under national security grounds may hinder cross-border transactions. Therefore, governments should establish transparent procedures to address these hurdles and provide clear expectations for private actors aiming to engage in cross-border transactions.

In Part I, this Note provides background information concerning the rising significance of data in private enterprises and national security. Part II of this Note introduces the use of national security exceptions under international trade and investment agreements, as well as the United States' domestic legal mechanism in determining and enforcing U.S. policies with regard to foreign investment. In Part III, this Note explores the lack of restraint in employing national security exception policy in the area of foreign investment in American businesses that possess significant private user data. Part IV discusses how CFIUS, the central mechanism in dealing with national security threats concerning foreign investment, lacks transparency and accountability and therefore may hinder cross-border transactions. Lastly, Part V proposes measures that provide greater transparency and accountability to CFIUS and consideration of data-localization law as a solution to facilitate foreign investment in American businesses of special concern.

9. *Id.*

10. Greg Roumeliotis, *U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns*, REUTERS, https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial-idUSKBN1ER1R7 (Jan. 2, 2018, 1:36 PM). *See, e.g.*, Echo Wang & Chibuike Oguh, *Grindr's Chinese Owner Says To Sell Social Media App for $608 Mln*, REUTERS, https://www.reuters.com/article/us-grindr-m-a-investors-exclusive-idUSKBN20T0IR (Mar. 5, 2020, 9:46 PM).

11. *See infra* Part III.B.

I. PRIVATE DATA AND NATIONAL SECURITY CONCERNS

Data is arguably a new commodity in the twenty-first century.[12] There are currently estimated over five billion internet users worldwide.[13] The collection of personal data has become a ubiquitous practice for internet-based service businesses.[14] As user-data gathering becomes the norm in digital private enterprises, the practice raises national security concerns as interested foreign actors may gain control over private data by gaining control of private enterprises.

"Private data" gathered by businesses can be far-reaching and include various categories of data.[15] While certain data, such as health records, social security information, and banking details, are considered as most sensitive information, other private data may be categorized differently due to the way it is monetized.[16] For instance, a business might collect private data regarding social media posts and geolocations, but such a business may monetize these private data differently than banking details collected online.[17] Businesses may also further collect information on consumers' engagement on their web platforms as well as consumers' attitudinal data.[18] Social media businesses, like Facebook, collect a large amount of personal data from their users on all of the content created by each user, such as posts and videos.[19] Facebook also collects users' usage data, networks and connections, and engagement in its services, among other metrics.[20]

This Note focuses on challenges that specifically pertain to private user data collected by private enterprises rather than data collected by government entities. Researchers estimate that the amount of data created by business enterprises will continue to increase due to the rise of cloud storage and other

12. Manisha Patel, *Is Data Our Most Valuable Commodity? 2020 Data Trends*, THE FINTECH TIMES (Feb. 3, 2020), https://thefintechtimes.com/data-2020-trends/; Mark Allinson, *How Has Data Become the World's Most Valuable Commodity?*, ROBOTICS & AUTOMATION NEWS (July 22, 2021), https://roboticsandautomationnews.com/2021/07/22/how-has-data-become-the-worlds-most-valuable-commodity/44267/; Kara Nortman, *Data Is the World's Most Valuable (and Vulnerable) Resource*, TECHCRUNCH (Mar. 4, 2021, 2:16 PM), https://social.techcrunch.com/2021/03/04/data-is-the-worlds-most-valuable-and-vulnerable-resource/.

13. *World Internet Users and 2022 Population Stats*, INTERNET WORLD STATS, https://www.internetworldstats.com/stats.htm (last visited Feb. 23, 2023).

14. Lance Whitney, *Data Privacy Is a Growing Concern for More Consumers*, TECHREPUBLIC (Aug. 17, 2021, 10:47 AM), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

15. Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/.

16. *Id.*

17. *Id.*

18. Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (Nov. 21, 2022).

19. *See Privacy Policy*, META, https://www.facebook.com/about/privacy (Jan. 1, 2023).

20. *Id.*

computing platforms.[21] While in 2015 business enterprises created less than thirty percent of data, one study by International Data Corporation estimated that by 2025 this figure will grow to nearly sixty percent.[22] With the rapid development of the Internet of Things devices, observers also argue that we have entered a new data age as we continue to integrate digital devices into our daily lives,[23] and that private data generated by these devices have become a key contributor to data growth.[24] It is worth noting that private entities bear the burden and responsibility of managing the majority of private data generated online.[25] The impact of data breaches and misuse of private data increases as private businesses continue to collect more and more data.

Due to the unprecedented amount of private data gathered by private enterprises, control of these business enterprises by interested foreign actors raise national security concerns. On a broader policy level, the central challenge that governments must confront is resolving the conflict between the great latitude that private enterprises enjoy in gathering and controlling private data and defense against national security threats posed by the potentially questionable use of private data.

A third party may use private user data in a variety of ways that impede national security. Take, for instance, Cambridge Analytica's abuse of user information gathered from Facebook.[26] In 2018, news reports surfaced regarding Cambridge Analytica's practice of gathering the private data of Facebook users via Facebook quizzes and questionnaires and obtaining insight into users' online habits.[27] The company reportedly gathered up to eighty-seven million Facebook users' online information.[28] Abuse of such data rises to a national security concern as malicious actors used the information gathered by Cambridge Analytica and reportedly interfered with U.S. domestic campaigns and foreign

21. DAVID REINSEL, JOHN GANTZ & JOHN RYDNING, DATA AGE 2025: THE EVOLUTION OF DATA TO LIFE-CRITICAL 9 (2017), https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf.

22. *Id.*

23. *Id.*; Irfan Saif, Sean Peasley & Arun Perinkolam, *Safeguarding the Internet of Things: Being Secure, Vigilant, and Resilient in the Connected Age*, 17 DELOITTE REV. 101, 101 (2015), https://www2.deloitte.com/content/www/us/en/insights/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.

24. REINSEL ET AL., *supra* note 21, at 11 ("Today, the number of embedded system devices feeding into datacenters is less than one per person globally, and over the next 10 years, that number will increase to more than four per person.").

25. *Id.* at 21 (noting that business enterprises bear the burden and responsibility of managing more than ninety-seven percent of the global datasphere).

26. Mark Scott & Annabelle Dickson, *Cambridge Analytica Created Own Quizzes To Harvest Facebook Data*, POLITICO (Apr. 17, 2018, 1:00 PM), https://www.politico.eu/article/cambridge-analytica-facebook-data-brittney-kaiser-privacy/.

27. *Id.*

28. *Id.* A whistleblower indicated that Cambridge Analytica built models to exploit the data gathered from Facebook that could profile U.S. individual voters with the goal of targeting these voters with personalized political advertisements. *See How Cambridge Analytica Turned Facebook 'Likes' into a Lucrative Political Tool*, THE GUARDIAN (Mar. 17, 2018), https://theguardian.com/technology/2018/mar/17/facebook-cambridge-analytical-kogan-data-algorithm.

campaigns like Brexit.[29] Further, congressional hearings revealed that Russian intelligence services may have had access to the data harvested by Cambridge Analytica.[30]

II. BACKGROUND ON NATIONAL SECURITY EXCEPTIONALISM AND U.S. NATIONAL SECURITY MECHANISMS FOR FOREIGN INVESTMENT

Foreign investment aiming to obtain control over private enterprises possessing significant private user data poses a special area of concern to governments. The United Nations has observed that numerous countries have increasingly addressed national security–related concerns in their investment policies.[31] Further, there is a rising concern over the economic and security implications of the growing presence and investment activities of firms that are owned or controlled by foreign governments.[32]

International agreements and bilateral treaties between countries may address national security concerns. The United States addresses national security concerns arising from the merger and acquisition of American private businesses by foreign entities through a multiagency mechanism under the CFIUS. In a national emergency, the President may also impose measures regarding economic transactions under the International Emergency Economic Powers Act.[33]

A. NATIONAL SECURITY EXCEPTIONALISM UNDER INTERNATIONAL AGREEMENTS

International investment treaties have promulgated an international investment legal regime that provides for national security exceptions to protect the host state's interests.[34] National security exceptions remove governments' obligations under binding international trade and investment agreements when specific conditions are met so that governments can protect their national security interests. While historically "national security" has been linked to the physical military and territorial protection of one nation, national security under international investment agreements is often broadly determined by the

29. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; *see also* Gillian Tett, *Trump, Cambridge Analytica and How Big Data Is Reshaping Politics*, FIN. TIMES (Sept. 28, 2017), https://www.ft.com/content/e66232e4-a30e-11e7-9e4f-7f5e6a7c98a2.

30. *Cambridge Analytica Shared Data with Russia: Whistleblower*, YAHOO! NEWS (May 16, 2018), https://news.yahoo.com/cambridge-analytica-shared-data-russia-whistleblower-151416794.html.

31. JAMES K. JACKSON, CONG. RSCH. SERV., RS21857, FOREIGN DIRECT INVESTMENT IN THE UNITED STATES: AN ECONOMIC ANALYSIS 12 (2017).

32. *Id.*

33. *See infra* Part II.C.

34. *See* Ji Ma, *International Investment and National Security Review*, 52 VAND. J. TRANSNAT'L L. 899, 902 (2019).

governments themselves,[35] and international tribunals have rejected that it only refers to military actions and war.[36] Due to such a broad definition of national security, countries often take the approach of both developing a screening system to review the appropriateness of foreign investment before the establishment of an investment relationship and enacting national security exception clauses in the investment treaties.[37]

Article XXI of the General Agreement on Tariffs and Trade (GATT) specifies that nothing in the GATT should be construed[38]

> (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests
>
> > (i) relating to fissionable materials or the materials from which they are derived;
> >
> > (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;
> >
> > (iii) taken in time of war or other emergency in international relations.

The language of "which it considers necessary" is arguably self-judging, based on the plain meaning of the language. This self-judging nature of the national security exception under Article XXI has raised further debates.

While the initial purpose of permitting the national security exception was to provide policy space for the member state under exceptional emergencies,[39] the self-judging nature of the exception may provide grounds for member states to invoke it without judicial review.[40] Scholars have noted that Article XXI, in effect, has been largely conceived in the GATT/WTO history as unenforceable due to its ambiguity and lack of objective standard on what constitutes "essential security interests."[41] Members of the WTO have shown self-restraint in invoking national security as a justification for trade restrictions and were eager to avoid any related disputes or to settle disputes outside of the WTO body for over seven decades, until recently.[42]

In 2016, Ukraine filed the first of a series of cases with the WTO panel disputing the national security exception under Article XXI against Russia regarding its restriction on traffic in transit from Ukraine, through Russia, to

35. *Id.* at 907.

36. *Id.* at 908.

37. *Id.* at 909 (examining in the context of the United States-Argentina Bilateral Investment Treaty).

38. General Agreement on Tariffs and Trade, art. XXI(b), Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194, 266.

39. Ji Yeong Yoo & Dukgeun Ahn, *Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security*, 19 J. INT'L ECON. L. 417, 429 (2016).

40. *Id.* at 427–28.

41. *Id.* at 426.

42. Peter Van den Bossche & Sarah Akpofure, *The Use and Abuse of the National Security Exception Under Article XXI(b)(iii) of the GATT 1994* 2–4 (World Trade Inst., Working Paper No. 03/2020, 2019), https://www.wti.org/media/filer_public/50/57/5057fb22-f949-4920-8bd1-e8ad352d22b2/wti_working_paper_03_2020.pdf.

Kazakhstan and other countries.[43] On April 26, 2019, the WTO's Dispute Settlement Body adopted its first report examining the nature and scope of the national security exception of Article XXI in response to the dispute between Ukraine and Russia.[44] The report concluded that when a member claims a national security measure necessary to protect its interest, the WTO panel can review the measure.[45] It further found that Russia's invocation of a national security concern was legitimate under subsection (b)(iii), considering the state of affairs between Russia and Ukraine.[46]

Against the backdrop of the controversies surrounding Article XXI of the GATT, bilateral investment treaties have taken a different approach in incorporating a national security exception provision.[47] The simplest version of the national security exception clause, as exemplified in the 2004 U.S. Model Bilateral Investment Treaty (U.S. Model BIT), has become the standard.[48] The national security exception provision provided under the U.S. Model BIT is similar to GATT Article XXI; however, it further broadens the scope of the security exception clause.[49]

A national security exception provision analogous to Article XXI of the GATT also exists under Article XIV of the General Agreement on the Trade of Services (GATS), which binds all WTO members.[50] As Article XXI of the GATT and Article XIV of GATS are nearly identical, the application of the national security exception under GATS would likely fare similarly under the WTO panel.[51]

Domestically, the power to address national security concerns regarding international trade and investment is almost exclusively granted to the Executive. Even though the President's action in restricting trade under national security concerns would be subject to Article XXI of the GATT, institutional scrutiny in Geneva poses "little threat of meaningful discipline over the President's actions,"[52] as the United States could claim that its actions are protected by the national security exception discussed above.

---

43. *Id.* at 4.

44. *Id.*

45. William Alan Reinsch, *The WTO's First Ruling on National Security: What Does It Mean for the United States?*, CTR. FOR STRATEGIC & INT'L STUD. (Apr. 5, 2019), https://www.csis.org/analysis/wtos-first-ruling-national-security-what-does-it-mean-united-states.

46. *Id.*

47. *See* Yoo & Ahn, *supra* note 39, at 436.

48. *Id.* at 438.

49. *Id.* at 437–38; U.S. Model Bilateral Investment Treaty, art. 18 (Off. of the U.S. Trade Representative 2004), https://ustr.gov/archive/assets/Trade_Sectors/Investment/Model_BIT/asset_upload_file847_6897.pdf ("Nothing in this Treaty shall be construed . . . to require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests . . . .").

50. Alexander R. Kerr Alvarez, *Dancing into Conflict: TikTok, National Security and the WTO*, EDINBURGH STUDENT L. REV. (Apr. 12, 2021), https://www.eslr.ed.ac.uk/2021/04/12/dancing-into-conflict-tiktok-national-security-and-the-wto/.

51. *Id.*

52. Kathleen Claussen, *Trade's Security Exceptionalism*, 72 STAN. L. REV. 1097, 1130–31 (2020).

B. COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

In the 1970s, the United States became increasingly concerned with the relative lack of power the government had to review foreign transactions within the United States as foreign nations' economies rose to global prominence.[53] In response, President Gerald Ford issued Executive Order 11,858 and established CFIUS in 1975.[54] CFIUS's primary responsibility is to monitor the "impact of foreign investment in the United States, both direct and portfolio, and for coordinating the implementation of United States policy on such investment."[55] While the creation of CFIUS was a significant step in enhancing the United States' investment security, CFIUS met sporadically in the first five years of its inception due to the reduced public concern over investment by foreign nations such as the OPEC countries.[56]

However, by the late 1980s, concerns regarding American companies being the acquisition target of foreign companies became widespread.[57] In 1988, to address these concerns, Congress enacted the Exon-Florio Amendment that created section 721 of the Defense Production Act of 1950.[58] Under the Exon-Florio Amendment, Congress delegated to the President the power to make investigations to determine "effects on the national security of mergers, acquisitions, and takeovers proposed or pending."[59] The Exon-Florio Amendment also permitted the President to take "such action for such time" as the President considers appropriate to suspend or prohibit any acquisition, merger, or takeover.[60] Soon after Congress passed the Exon-Florio Amendment, President Ronald Reagan issued Executive Order 12,661, which delegated his authority under the Amendment to CFIUS.[61]

Since the Exon-Florio Amendment, Congress has made several adjustments to CFIUS, including specifying the scope of CFIUS's review power[62] and adding additional factors the President must consider in

53. Matthew Aglialoro, *Defend and Protect: National Security Restrictions on Foreign Investment in the United States*, 83 U. CIN. L. REV. 1261, 1269 (2015).

54. Exec. Order No. 11,858, 40 Fed. Reg. 20263, 20263 (May 7, 1975).

55. *Id.*

56. Heath P. Tarbert, *Modernizing CFIUS*, 88 GEO. WASH. L. REV. 1477, 1484 (2020).

57. *Id.* at 1485–86.

58. Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat. 1107, 1425 (codified as amended at 50 U.S.C. app. § 2170).

59. *Id.*

60. *Id.*

61. Exec. Order No. 12,661, 3 C.F.R. 618, 620–21 (1989).

62. *See* National Defense Authorization Act for Fiscal Year 1993, Pub. L. No. 102-484, § 837, 106 Stat. 2315, 2463–65 (1992) (codified as amended at 50 U.S.C. app. § 2170(b)); 50 U.S.C. app. § 2170 (2000); Chang Liu, Ralls v. CFIUS*: The Long Time Coming Judicial Protection of Foreign Investors' Constitutional Rights Against Government's National Security Review*, 15 J. INT'L BUS. & L. 361, 365 (2016) ("[The National Defense Authorization Act for Fiscal Year 1993] made three [significant] changes. First, the amendment made it mandatory for CFIUS to investigate any transaction involving a foreign government, if that transaction could affect national security. Second, it requires the President to report to Congress the results of any CFIUS investigation, regardless of whether the president decided to take action. Finally, the amendment added two new factors that the President could consider in determining whether a transaction posed a threat . . . .").

determining whether a transaction poses a national security threat.[63] In 2007, Congress enacted the Foreign Investment and National Security Act of 2007 (FINSA), which formally established CFIUS as an entity with defined, expanded members[64] and strengthened congressional oversight.[65] Currently, CFIUS is an interagency committee that consists of nine members, including the Secretary of the Treasury, who serves as its Chairperson; the Secretaries of State, Defense, Homeland Security, Commerce, and Energy; the Attorney General; the United States Trade Representative; and the Director of the Office of Science and Technology Policy.[66] "The Secretary of Labor and the Director of National Intelligence serve as ex officio members of the [C]ommittee."[67]

As the President utilizes CFIUS's broad statutory authority to address national security challenges posed by foreign investments, emerging challenges posed by foreign investments and transactions involving private user data require CFIUS to "modernize" to be able to address these challenges in the new digital age.[68] To address the challenges and limits faced by CFIUS, in 2018, Congress passed the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) with bipartisan support. FIRRMA transformed CFIUS by expanding its mandate, significantly increasing its range of covered transactions, including minority investments, and turning it into a quasi-agency with expanded staff and funding.[69]

Among several changes critical to the technology data industry is the expansion of CFIUS's scope to include reviewing noncontrolling investment in American businesses in critical technology, critical infrastructure, or American businesses that collect sensitive data on U.S. citizens.[70] Prior to FIRRMA, CFIUS had the authority to review mergers, acquisitions, or takeovers by or with any foreign person that could result in foreign control of U.S. business.[71] FIRRMA specifically expanded CFIUS's authority to include noncontrolling investment in U.S. businesses that "maintain[] or collect[] sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[72] Such investment would fall under CFIUS's purview if the

63. Liu, *supra* note 62, at 364.

64. *See generally* Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246; *see also* 50 U.S.C. app. § 2170(a)–(b), (f)(11), (l)–(m) (2012); Tarbert, *supra* note 56, at 1490–92 (noting that FINSA made several major changes to CFIUS).

65. Tarbert, *supra* note 56, at 1490–92.

66. *CFIUS Overview*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview (last visited Feb. 23, 2023).

67. JAMES K. JACKSON, CONG. RSCH. SERV., IF10177, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (2019).

68. Tarbert, *supra* note 56, at 1492–93.

69. Evan J. Zimmerman, Note, *The Foreign Risk Review Modernization Act: How CFIUS Became a Tech Office*, 34 BERKELEY TECH. L.J. 1267, 1285 (2019).

70. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, §§ 1703–1728, 132 Stat. 2174, 2174–2207 (codified as amended at 50 U.S.C. § 4565).

71. *See* 50 U.S.C. § 4565(a)(4)(B)(i).

72. *Id.* § 4565(a)(4)(B)(iii)(III).

investment in the American business of concern would afford the foreign person any other fundamental decisionmaking rights regarding "the use, development, acquisition, safekeeping, or release of sensitive personal data of United States citizens maintained or collected by the United States business."[73] CFIUS's jurisdiction over these cases would be "both on the attribute[] of the U.S. business as well as the nature of the rights the investor would enjoy."[74] Part IV.A further explores the implications of the categories of data under "sensitive personal data" as defined under FIRRMA.

Procedurally, the first step of CFIUS review is a declaration filing with basic information.[75] The declaration is a voluntary process where parties may submit a short-form declaration notifying CFIUS of a covered transaction.[76] If the parties can receive a "safe harbor" letter, CFIUS is limited to "subsequently initiating a review of a transaction except in certain limited circumstances."[77] FIRRMA also mandates the filing of a declaration for a covered transaction where a foreign government is acquiring "substantial interest" in certain U.S. businesses and specific transactions where critical technologies are involved.[78] Prior to the declaration filing, there is also an informal stage where individual CFIUS members may conduct an unofficial review.[79]

In assessing national security risk, CFIUS evaluates: "(1) the threat, which involves an assessment of the intent and capabilities of the acquirer; (2) the vulnerability, or an assessment of the aspects of the U.S. business that could impact national security; and (3) the potential national security consequences if the vulnerabilities were to be exploited."[80] If CFIUS determines that the investment poses no national security issue under the declaration review, then the transaction can proceed as normal.[81] If there is a risk or the risk is not resolved by a mitigation agreement, CFIUS may initiate a unilateral national security review.[82] If the reviewed parties are not able to pass the review phase due to triggering factors, the next step for CFIUS is to conduct a national security investigation.[83] "During [the] review or an investigation, CFIUS . . . [has] the

73. *Id.* § 4565(a)(4)(D)(i)(III)(aa).

74. Tarbert, *supra* note 56, at 1505.

75. *CFIUS Overview*, *supra* note 66.

76. JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 19 (2020).

77. *CFIUS Overview*, *supra* note 66.

78. JACKSON, *supra* note 76, at 19–20 ("The regulations specify a voting interest (direct or indirect) threshold for 'substantial interest' of 25% between a foreign person and U.S. business and 49% or greater between a foreign government and foreign person. . . . Critical technologies are defined as those that are (1) used in a U.S. business's activity in the specified industries, or (2) designed by the U.S. business specifically for use in those industries.").

79. *Id.* at 14.

80. *Id.* at 11.

81. *Id.* at 22.

82. *Id.* at 22–23.

83. Liu, *supra* note 62, at 368 ("[This step is triggered] (i) if a national security threat found during the Review was not mitigated, either prior to the Review or through a mitigation agreement; (ii) if the transaction

authority to negotiate, impose, or enforce any agreement or condition with the parties to [the] transaction in order to mitigate any threat to U.S. national security."[84] Lastly, when extraordinary measures are required, it is the President, rather than CFIUS, who may act on the advice of the Committee through the power granted under section 721 of the Defense Production Act of 1950.[85]

C. INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT

To regulate economic transactions concerning national security, another pertinent legal mechanism that the U.S. government has also relied on is the International Emergency Economic Powers Act (IEEAP). Under IEEPA, the President possesses broad authority to regulate a variety of economic transactions following a declaration of national emergency.[86]

Most of the actions taken under IEEPA have involved blocking transactions and freezing assets.[87] Under section 203 of IEEPA, upon the declaration of a national emergency, the President may

> investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal . . . or dealing in . . . or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States.[88]

While Presidents have historically used the IEEPA for U.S. sanctions programs, scholars have observed that former President Trump used IEEPA powers contrary to its legislative intent with expansive application and greater frequency to further foreign policy objectives.[89]

---

results in U.S. assets being controlled by a foreign government; or (iii) if the transaction involves the transfer of a U.S. asset that is deemed to be any form of 'critical infrastructure' without mitigations for the risk.").

84. JACKSON, *supra* note 76, at 23.

85. Liu, *supra* note 62, at 368.

86. *See* 50 U.S.C. § 1701; CHRISTOPHER A. CASEY, DIANNE E. RENNACK & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 10 (2022) ("[The President may exercise powers] to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat.").

87. CASEY ET AL., *supra* note 86, at 24.

88. 50 U.S.C. § 1702(b).

89. Alicia Faison, Note, *TikTok Might Stop: Why the IEEPA Cannot Regulate Personal Data Privacy and the Need for a Comprehensive Solution*, 16 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 115, 119 (2021); Claussen, *supra* note 52, at 1119 ("Since its inception, IEEPA has been used primarily for the U.S. sanctions program.").

III. NEW NATIONAL SECURITY CHALLENGES TO THE LIBERAL ECONOMIC ORDER

Even though the intersection between national security and trade policies has long been contentious, the current trade regime has managed to cabin the issue.[90] However, scholars note a proliferation of WTO disputes over national security measures in recent years.[91] There is a growing consensus that the use of national security exception policies has become widespread and that these policies are increasingly likely to conflict with trade and investment rules.[92] Specifically, the self-judging nature of the national security exception clause is colliding with the liberal economic order, and such conflicts are no longer manageable by the current mechanism.[93]

In *The New National Security Challenge to the Economic Order*, Professor J. Benton Heath argues that the expanding number of issues confronted by states has challenged the traditional theory, which assumes that mutual restraints from states will enforce the boundary in overusing the national security exception.[94] Further, the alternative approach of having an adjudicative body such as the WTO to resolve these disputes has failed.[95] Professor Heath asserts that the "collision between trade and security cannot be managed either by law or politics alone,"[96] and that "the rise of the new national security poses a potentially fatal challenge to these two models and demands that we consider solutions that fall between adjudication and politics."[97] Because states have incentives to utilize national security exception measures to their advantage in facing new challenges in areas of "terrorism, climate change, cyber threats, and economic insecurity,"[98] this practice challenges the global economic order and "require[s] changes to the trade and investment system's design."[99]

While Professor Heath points out cybersecurity as one of the new challenges that raise national security concerns, there are other challenges in the cyberspace, especially surrounding the use of private data as discussed in Part I. Worldwide, governments are actively asserting "digital sovereignty" with respect to how and where data is stored and who has access to it.[100]

---

90. Claussen, *supra* note 52, at 1136.

91. Simon Lester & Inu Manak, *A Proposal for a Committee on National Security at the WTO*, 30 DUKE J. COMPAR. & INT'L L. 267, 271 (2020).

92. Heath, *supra* note 2, at 1020.

93. *Id.* at 1024–26.

94. *Id.* at 1026.

95. *Id.*

96. *Id.*

97. *Id.* at 1027.

98. *Id.* at 1029.

99. *Id.*

100. *See, e.g.*, Linsdey R. Sheppard, Erol Yayboke & Carolina G. Ramos, *The Real National Security Concerns over Data Localization*, CTR. FOR STRATEGIC & INT'L STUD. 1 (July 23, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210723_Sheppard_DataLocalization.pdf?en2io56tR_AVK4Ts6yzoHoafKr354j5t.

The United States has addressed national security challenges posed by foreign investment surrounding private businesses that gather significant private data. By examining the regulations and actions taken by the Trump and Biden Administrations in this area, this Note finds support for Professor Heath's argument that the assumption of mutual restraints in employing national security exceptions by states is no longer applicable, and that international adjudicative bodies such as the WTO have not provided adequate remedies.

A. WEAPONIZING THE NATIONAL SECURITY EXCEPTION UNDER THE TRUMP ADMINISTRATION

Due to the absence of a bilateral investment treaty between the United States and China, enacting economic actions under national security grounds from both countries is arguably only subject to relevant WTO laws and the self-restraint of the two countries. Running on the nationalistic rhetoric of "Making America Great Again" and a protectionist economic platform,[101] former President Trump employed anti-China rhetoric and directed targeted trade sanctions against China starting in 2018.[102] Self-restraint in employing national security grounds to restrict trade and investment has diminished under this context.

CFIUS is the central mechanism of addressing the national security challenges posed by Chinese investment in American companies possessing significant private user data. While the President may regulate economic transactions with regard to national security issues under IEEPA,[103] challenges posed by the use of private data may not be appropriately addressed under IEEPA because the ban on acquiring private companies with private data may violate IEEPA's carve-out on information materials.[104] In the case of TikTok, former President Trump issued an executive order pursuant to his IEEPA power addressing the U.S. operation of TikTok.[105] Pursuant to the executive order, the Commerce Department issued restrictions on TikTok, which included a first step of an app-store ban and a second step of blocking its operation in the United States.[106] TikTok challenged these restrictions in *TikTok Inc. v. Trump*.[107] The U.S. District Court for the District of Columbia granted ByteDance's, TikTok's parent company, request for a preliminary injunction against the app-store ban,

101. Chi Hung Kwan, *The China–US Trade War: Deep-Rooted Causes, Shifting Focus and Uncertain Prospects*, 15 ASIAN ECON. POL'Y REV. 55, 60 (2020).

102. *See* Andrew Mullen, *US-China Trade War Timeline: Key Dates and Events Since July 2018*, S. CHINA MORNING POST (Aug. 29, 2021, 8:00 PM), https://www.scmp.com/economy/china-economy/article/3146489/us-china-trade-war-timeline-key-dates-and-events-july-2018.

103. *See supra* Part II.C.

104. Faison, *supra* note 89.

105. Exec. Order No. 13,942, 85 Fed. Reg. 48637, 48637 (Aug. 11, 2020).

106. *Regulatory Actions Against TikTok*, *supra* note 4, at 126.

107. TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 76 (D.D.C. 2020).

noting that TikTok is likely to fall under the exception to the President's IEEPA authority.[108]

The Trump Administration began its parallel action against ByteDance under CFIUS as early as November 2019.[109] On August 14, 2020, former President Trump issued an executive order to unwind ByteDance's acquisition of Musical.ly, a video-sharing application acquired by ByteDance that provided much of TikTok's early base of U.S. users.[110] The order further set a ninety-day deadline for ByteDance to divest all its interests and rights in assets or property used to support the operation of TikTok in the United States, as well as any data obtained or derived from TikTok users in the United States.[111] The United States has since then been deeply involved in the sale and transfer of ownership of TikTok, including the close scrutiny of takeover discussions with major U.S. corporations like Microsoft and Oracle.[112] Under President Biden, the executive order from former President Trump has not been enforced.[113] The Biden Administration is in active negotiation with ByteDance, and the two parties may soon reach a preliminary agreement to resolve the national security concerns.[114] However, the specifics of the agreement are still confidential.[115]

The Trump Administration further utilized CFIUS to order the unwinding or divestment of other Chinese investments in American businesses that have gathered significant personal data. In fact, the first public announcement over concerns of data security involving a Chinese buyer and an American target was CFIUS's decision over Ant Financial's acquisition of MoneyGram International Inc. in 2018.[116] CFIUS rejected Ant Financial's filing to acquire MoneyGram, a U.S. money transfer company.[117] The two companies decided to terminate their deal after CFIUS rejected their proposal to mitigate national security concerns over the safety of data that can be used to identify U.S. citizens.[118]

Under the Trump Administration, actions against other Chinese investments in American businesses of interest persisted. American social media

108. *Id.*; *see also Regulatory Actions Against TikTok*, *supra* note 4, at 127–28.

109. *Regulatory Actions Against TikTok*, *supra* note 4, at 129.

110. Order of August 14, 2020: Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297, 51297–99 (Aug. 19, 2020).

111. *Id.* at 51297.

112. *Regulatory Actions Against TikTok*, *supra* note 4, at 129–30.

113. John D. McKinnon & Alex Leary, *TikTok Sale to Oracle, Walmart Is Shelved as Biden Reviews Security*, WALL ST. J., https://www.wsj.com/articles/tiktok-sale-to-oracle-walmart-is-shelved-as-biden-reviews-security-11612958401 (Feb. 10, 2021, 5:40 PM).

114. Lauren Hirsch, David McCabe, Katie Benner & Glenn Thrush, *TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain*, N.Y. TIMES (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html.

115. *Id.*

116. David J. Lavan, Harvey Jay Cohen & Patrick R. Schlembach, *MoneyGram-Ant Financial Transaction the Latest Casualty of CFIUS's Increased Scrutiny of Chinese Deals; CFIUS Interprets "National Security" To Include Data-Security, Fails To Approve Deal*, NAT'L L. REV. (Jan. 18, 2018), https://www.natlawreview.com/print/article/moneygram-ant-financial-transaction-latest-casualty-cfius-s-increased-scrutiny.

117. Roumeliotis, *supra* note 10.

118. *Id.*

networking company PatientsLikeMe provides a digital platform where patients can connect with each other and share information about their health conditions.[119] In 2017, China-based iCarbonX invested approximately $100 million in PatientsLikeMe, a significant minority investment.[120] However, in 2019, CFIUS ordered China-based iCarbon X to sell its shares in PatientsLikeMe.[121] In 2020, CFIUS ordered Beijing Kunlun Tech Co. Ltd., a Chinese gaming company, to sell its 98.59% stake in Grindr, a U.S.-based company that claims to be the world's largest social networking app for the LGBTQ community.[122] While CFIUS did not disclose its concern regarding Kulun's ownership of Grindr, a news report noted that it is likely due to the United States' increasing concern over the safety of data handled by app developers, especially when it involves U.S. military or intelligence personnel.[123] The media has reported that Grindr had given engineers based in Beijing access to the sensitive personal data of millions of U.S. users, including private messages and HIV status.[124]

B. ESTABLISHMENT OF NORMS UNDER THE BIDEN ADMINISTRATION

CFIUS actions that took off under the Trump Administration are unlikely to cool off under the Biden Administration. According to current and former officials, the expansive evolution of CFIUS under the Trump Administration is likely to be the "linchpin" in President Biden's plan to compete with China.[125] Noting the high profile that CFIUS has played amid the ongoing trade tension with China under the Trump Administration, U.S. practitioners observe that CFIUS work is likely to continue to operate rigorously.[126]

An important indicator of the Biden Administration's approach to foreign investment in American businesses involving private data is the Administration's decision to extend Executive Order 13,873 ("EO 13,873"), first issued under former President Trump. In May 2019, former President Trump issued EO 13,873, in which he declared a national emergency, citing that

119. *CFIUS Mitigation: iCarbonX and PatientsLikeMe Inc*, THE TRADE PRAC. (June 25, 2019), https://www.tradepractitioner.com/2019/06/icarbonx-patientslikeme/.

120. *Id.*

121. *CFIUS Mitigation: iCarbonX and PatientsLikeMe Inc*, *supra* note 119.

122. Wang & Oguh, s*upra* note 10.

123. *Id.*

124. Zack Whittaker, *Grindr Sold by Chinese Owner After US Raised National Security Concerns*, TECHCRUNCH (Mar. 6, 2020, 10:06 AM), https://social.techcrunch.com/2020/03/06/grindr-sold-china-national-security/.

125. Alex Leary & Katy Stech Ferek, *Panel Gets Key Role in China Fight*, WALL ST. J., July 8, 2021, at A4.

126. Farhad Jalinous, Karalyn Mildorf & Keith Schomig, *CFIUS Set To Continue Careful Scrutiny Under Biden Administration*, WHITE & CASE LLP (July 30, 2021), https://www.whitecase.com/publications/insight/us-ma-2021/cfius-biden-administration; Donald F. McGahn II, Schuyler J. Schouten & Chad R. Mizelle, *Rigorous CFIUS Reviews Will Continue Under Biden: How To Prepare*, BLOOMBERG L. (Apr. 9, 2021, 1:01 AM), https://news.bloomberglaw.com/us-law-week/rigorous-cfius-reviews-will-continue-under-biden-how-to-prepare; *CFIUS in the Biden Administration*, COVINGTON & BURLING LLP (Jan. 29, 2021), https://www.cov.com/en/news-and-insights/insights/2021/01/cfius-in-the-biden-administration.

the acquisition or use of U.S. information and communications technology or services by foreign adversaries constitutes an unusual and extraordinary threat to U.S. national security.[127] Under the order, the Department of Commerce may block, unwind, or condition transactions involving information and communication technology and services (ICTS) "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of [a] foreign adversar[y]."[128] "ICTS" includes "hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means."[129]

Just one day before President Biden assumed office, the Department of Commerce published an interim rule implementing EO 13,873 by former President Trump.[130] The rule lists six main types of ICTS transactions, which include internet-connected software designed primarily for connecting and communication in use by greater than one million U.S. persons.[131] This would include social media and communication apps and ICTS products, of which greater than one million units have been sold to U.S. persons[132] and which include internet-enabled devices.[133]

While there may seem to be an overlap in the scope of work under CFIUS, the interim rule also addresses situations not covered by CFIUS, such as the national security implications of "a private person or entity merely using certain foreign produced goods and services."[134] Further, its language specifies that the rule does not apply to an ICTS transaction that CFIUS is "actively reviewing, or has reviewed, as a covered transaction . . . under section 721 of the Defense Production Act of 1950, as amended, and its implementing regulations."[135] However, an ICTS transaction that is separate from the transaction reviewed by CFIUS may be subject to review under this interim rule if it is "separate from, and subsequent to, a transaction for which CFIUS has concluded action under section 721."[136] The interim rule also specifies that the Secretary will determine "foreign adversaries" based on the executive order's purpose and revise as

127. Exec. Order No. 13,873, 84 Fed. Reg. 22689, 22689 (May 17, 2019).

128. *Id.*

129. *Id.* at 22691.

130. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909, 4914 (Jan. 19, 2021).

131. *Id.* at 4913.

132. *Id.*

133. John P. Barker, Ronald D. Lee, Soo-Mi Rhee, Nancy L. Perkins, Nicholas L. Townsend & Trevor G. Schmitt, *Beyond TikTok: Commerce Issues New CFIUS-Like Review Rule for Transactions Involving Information and Communications Technologies and Services*, ARNOLD & PORTER KAYE SCHOLER LLP (Feb. 4, 2021), https://www.arnoldporter.com/en/perspectives/advisories/2021/02/beyond-tiktok.

134. *Id.*

135. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. at 4914.

136. *Id.*

necessary.[137] Under this interim rule, six countries have been identified as "foreign adversar[ies]," including China.[138]

The Biden Administration continued this approach under EO 13,873. In Executive Order 14,034, President Biden rescinded several executive orders under the Trump Administration regarding measures taken under national security concerns on a transaction involving ICTS (including Executive Order 13,942, which banned TikTok), but reaffirmed EO 13,873 by asking the Secretary of Commerce to conduct an evaluation and further implement EO 13,873.[139] In the proposed rule pursuant to Executive Order 14,034, the Department of Commerce affirmed the approach taken under the Trump Administration and in fact broadened the scope of review.[140] Specifically, ICTS now would further encompass "connected software applications" targeting software that collect, process, or transmit data from devices via the internet.[141] The proposed rule is currently under the review of the Department and is pending further implementation.[142]

C. INTERNATIONAL DISPUTE MECHANISM IN RESPONSE

In the absence of bilateral treaties, members of the WTO rely on the institution as a forum for member states to resolve trade disputes under WTO's generally applicable rules. While traditional tariffs against Chinese exports would be under the WTO's purview—the United States and China have indeed approached the WTO mechanism to address the issue[143]—it is unclear as to whether the United States' restriction of Chinese investment in American private businesses possessing private user data is under the purview of the WTO.

China has claimed that the United States' restrictive action on TikTok was in violation of the WTO rules.[144] However, the dispute has not been formally submitted for review by the WTO. There is also controversy as to whether the WTO can prevent a U.S. President's order to unwind Chinese investment in TikTok. There is, first, a classification conundrum as to whether GATS applies

137. *Id.* at 4911.

138. The six countries identified as "foreign adversaries" are The People's Republic of China, including the Hong Kong Special Administrative Region (China); the Republic of Cuba (Cuba); the Islamic Republic of Iran (Iran); the Democratic People's Republic of Korea (North Korea); the Russian Federation (Russia); and Venezuelan politician Nicolás Maduro (Maduro Regime). *Id.*

139. *See generally* Protecting Americans' Sensitive Data from Foreign Adversaries, Exec. Order No. 14,034, 86 Fed. Reg. 31423 (June 11, 2021).

140. Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications, 86 Fed. Reg. 67379, 67380 (Nov. 26, 2021) (to be codified at 15 C.F.R. pt. 7).

141. *Id.* at 67380–81.

142. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. at 4909.

143. *US China Tariffs 'Inconsistent' with Trade Rules Says WTO*, BBC NEWS (Sept. 15, 2020), https://www.bbc.com/news/business-54168419.

144. *China Says U.S. TikTok, Wechat Bans Break WTO Rules*, REUTERS, https://www.reuters.com/article/usa-tiktok-ban-wto-idUSKBN26Q2LL (Oct. 5, 2020, 10:08 AM).

to the digital services that TikTok provides.[145] Second, China is unlikely to be able to bring a claim to WTO under the Trade-Related Aspects of Intellectual Property Rights (TRIPS) because it is unlikely to be applicable.[146] Even if services provided by TikTok were under the purview of the GATS, due to the lack of jurisprudence on the self-judging nature of national security exceptions, it is still highly contentious whether the United States properly invoked its national security exception ground. Such lack of predictability and stability signals a turn away from the consensus that the WTO is premised upon. As Professor Heath observes, "the unpredictability created by the new national security will continue to challenge the existing economic rules."[147]

IV. IMPACT OF U.S. POLICIES ON CROSS-BORDER TRANSACTIONS

Employing CFIUS to safeguard U.S. national security interests may hinder cross-border transactions due to its expansive authority coupled with a lack of transparency and accountability. While the "multilateral trading system and the United States program of bilateral commercial and investment treaties were founded in part on the conviction that deeper economic integration would mitigate conflicts and prevent world wars,"[148] the direction under the current regime headed by CFIUS is contradictory to this established liberal global economic order.

A. THE WIDE-REACHING DEFINITION OF "SENSITIVE PERSONAL DATA" CREATES UNCERTAINTY.

FIRRMA has expanded CFIUS's scope of review to include noncontrolling investment in U.S. businesses that maintain or collect "sensitive personal data."[149] A close examination of the definition of "sensitive personal data" reveals the wide-reaching power of CFIUS in this area. While China has been the central target in this regard, such a mechanism could have negative implications for other foreign investors.

The Treasury Department has clarified that "sensitive personal data," as stipulated under FIRRMA, first includes identifiable data collected by a U.S. business that targets sensitive U.S. government agencies.[150] Second, acknowledging that the volume of data itself sometimes matters, this category would also apply to a U.S. business that has maintained or collected the data of one million or more individuals (or with a demonstrated objective to do so), and

145. Sunanda Tewari, *The TikTok Controversy: Can WTO Prevent Bans?*, REGULATING FOR GLOBALIZATION (Sept. 1, 2020), http://regulatingforglobalization.com/2020/09/01/the-tiktok-controversy-can-wto-prevent-bans/?output=pdf.

146. *Id.*

147. Heath, *supra* note 2, at 1063.

148. *Id.* at 1047–48.

149. *See supra* Part II.B.

150. 31 C.F.R. § 800.241(a)(1)(i) (2021).

where the data will be an integrated part of the U.S. business's primary products or services, with respect to any of the following ten categories[151]: (1) financial data that could identify an individual's financial distress or hardship;[152] (2) consumer report data;[153] (3) data relating to health insurance;[154] (4) data relating to the health condition of an individual;[155] (5) "electronic communications, including email, messaging, or chat communications . . . if [the] primary purpose of [the] product or service is to facilitate third-party user communications";[156] (6) geolocation data;[157] (7) biometric data of an individual;[158] (8) data stored or processed for generating a government identification card;[159] (9) data concerning U.S. government personnel security clearance status;[160] or (10) "data in an application for a U.S. Government personnel security clearance or an application for employment in a position of public trust."[161] "Sensitive personal data" also includes the result of an individual's genetic test.[162]

The Department of Commerce's pending regulatory scheme uses a similar definition for "sensitive personal data" in regulating transactions involving U.S. business concerning ICTS transactions where parties to the transactions use, possess, or retain sensitive personal data.[163] The Department has defined "sensitive personal data" to include: (1) "personally identifiable information that is maintained or collected by a United States business operating in specific areas, and that is maintained or collected on over one million people over a twelve-month period," and (2) the "results of individual genetic testing."[164] The term "personally identifiable information" includes almost identical categories of information as the ten categories listed under the Treasury Department's regulation regarding "sensitive data" under CFIUS's review.[165]

The expansive scope of "sensitive personal data" under CFIUS and the Commerce Department regulation may create uncertainty and cast doubt on American investment transactions for international trade partners. It begs the question of what kind of data is excluded from "sensitive personal data." Without further clarification from administrative regulations, it seems that only

151. *Id.*
152. *Id.* § 800.241(a)(1)(ii)(A).
153. *Id.* § 800.241(a)(1)(ii)(B).
154. *Id.* § 800.241(a)(1)(ii)(C).
155. *Id.* § 800.241(a)(1)(ii)(D).
156. *Id.* § 800.241(a)(1)(ii)(E).
157. *Id.* § 800.241(a)(1)(ii)(F).
158. *Id.* § 800.241(a)(1)(ii)(G).
159. *Id.* § 800.241(a)(1)(ii)(H).
160. *Id.* § 800.241(a)(1)(ii)(I).
161. *Id.* § 800.241(a)(1)(ii)(J).
162. *Id.* § 800.241(a)(2).
163. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909, 4924 (Jan. 19, 2021).
164. *Id.* at 4912.
165. *See id.*

behavioral and attitudinal data generated by users would be excluded from the definition of "sensitive personal data."

Further, with the rise of the Internet of Things, businesses are shifting to turn everyday products into "smart devices" that continue collecting users' individual biometrics data. For instance, businesses are turning clothes into gadgets that collect consumers' biometric data,[166] and the wide use of wearables like the Apple Watch has transformed the personal fitness and health data collection process.[167] As everyday consumer products and products that gather private user data increasingly overlap, the expansive definition of "sensitive personal data" may cover a wide array of American businesses. This would mean that CFIUS and the Commerce Department would have expansive power to regulate foreign investment in businesses that previously would not be considered under national security concerns. This creates unpredictability for foreign investment in American businesses.

Acknowledging such expansive authority, the Treasury Department has promulgated regulations to limit the application of the expanded CFIUS review process for "excepted foreign states."[168] However, the exception is limited. Current excepted foreign states include only Australia, Canada, New Zealand, and the United Kingdom.[169]

B. CFIUS EXERCISES BROAD DISCRETION.

CFIUS possesses great discretion in its statutory scheme and decisionmaking process. Due to the broad authority delegated to CFIUS to initiate national security review, coupled with the inconsistent application of the CFIUS process to politically sensitive transactions, the CFIUS review process has been criticized for being overpoliticized and counterproductive.[170] The lack of transparency and the wide latitude of discretion afforded to CFIUS may hurt cross-border transactions by causing a lack of predictability and political stability for foreign investors.

As information filed with CFIUS is fully protected and classified, such a lack of transparency poses the first hurdle to gaining insight into CFIUS's decisionmaking process and considerations. Section 721 of the Defense Production Act of 1950 mandates confidentiality protections with respect to

166. David Pierce, *How Under Armour Plans To Turn Your Clothes into Gadgets*, WIRED (Jan. 5, 2016, 6:00 AM), https://www.wired.com/2016/01/under-armour-healthbox/.

167. Robbie Gonzalez, *Apple's Newest Watch Features Will Transform Heart Health*, WIRED (Dec. 6, 2018, 9:00 AM), https://www.wired.com/story/apple-watch-heart-monitoring-pros-and-cons/.

168. JACKSON, *supra* note 76, at 16.

169. *CFIUS Excepted Foreign States*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states (last visited Feb. 23, 2023).

170. Amy S. Josselyn, *National Security at All Costs: Why the CFIUS Review Process May Have Overreached Its Purpose*, 21 GEO. MASON L. REV. 1347, 1379 (2014).

information filed with CFIUS.[171] Further, information filed with the Committee is also exempted from disclosure under the Freedom of Information Act.[172]

Even though CFIUS decisions are subject to judicial review, unlike the measures and findings by the President that may be exempted,[173] there is still arguably minimal oversight over CFIUS's procedural review process. In the first case in which foreign investors rejected CFIUS's determination and the President's executive order, *Ralls Corp. v. Committee on Foreign Investment in the United States*, the Chinese-owned Ralls Corporation purchased four American companies that developed wind farms in Oregon.[174] CFIUS and the President found that the transaction posed a national security threat and ordered the reversal of Ralls's acquisition.[175] Ralls filed suit to invalidate the order and enjoin its enforcement, and the D.C. Circuit found that CFIUS's and the President's notice and the lack of disclosure of nonclassified evidence in the decision to reverse Ralls's acquisition deprived Ralls of its property right interest in violation of procedural due process.[176] However, all other aspects of CFIUS review procedures are completely outside the scope of judicial review.[177] The court in *Ralls* recognized a "basic degree of constitutional protection for private property," but the baseline is that the government should "disclose unclassified information that it relied on to prohibit foreign acquisitions."[178] As it stands, the government can still claim that it "relied on some classified evidence that could not be disclosed to the public [or] . . . [could] assert executive privilege as the Presidential Order was made based on national security."[179]

Further, the President is under no obligation to follow CFIUS's recommendation to suspend or prohibit investment, and the President may invoke executive authority upon concluding that other U.S. laws are inadequate or inappropriate to protect national security, supported by credible evidence that the foreign investment would "impair" national security.[180] The court therefore affirmed the President's sweeping power as granted under section 721 of the Defense Production Act of 1950, noting that it gives the President "broad latitude to engage in a retroactive review of closed deals and require and restrict action by the parties."[181]

171. *CFIUS Contact Information*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-contact-information (last visited Feb. 23, 2023).

172. *Id.*

173. Liu, *supra* note 62, at 386.

174. Ralls Corp. v. Comm. on Foreign Inv. in the U.S., 758 F.3d 296, 301 (D.C. Cir. 2014).

175. *Id.* at 301–02.

176. Liu, *supra* note 62, at 375.

177. *Id.*

178. *Id.* at 387.

179. *Id.*

180. JACKSON, *supra* note 76, at 23.

181. Hunter Deeley, Note, *The Expanding Reach of the Executive in Foreign Direct Investment: How* Ralls v. CFIUS *Will Alter the FDI Landscape in the United States*, 4 AM. U. BUS. L. REV. 125, 141 (2015); *see also*

CFIUS also possesses expansive power to reach past transactions. CFIUS has the authority to identify transactions that may pose a national security concern and take unilateral action, even where the parties involved have not affirmatively disclosed the transaction.[182] Therefore, companies may receive contact from CFIUS in "surprise."[183] Kunlun, for example, acquired a majority stake in Grindr in 2016 and bought out the remainder of the company in 2018 without submitting the transactions for CFIUS review.[184] Subsequently, the acquisition fueled privacy concerns in the United States with regard to users' privacy under the company's Chinese owner.[185] Kunlun was reportedly selling its stake in Grindr in 2020 upon CFIUS intervention.[186]

Considering the expansive scope of CFIUS's purview on foreign investment in American businesses possessing private data and its highly discretionary review process, such a national security scheme poses a significant challenge and unpredictability to foreign investors. Most investors opted out of challenging the federal government in U.S. court and simply complied with the authority.[187] A survey of Chinese investors who have some knowledge regarding CFIUS consider the process politicized and nontransparent, with a minority noting that they have abandoned contemplated investment in the United States due to concerns with CFIUS.[188]

V. PROPOSED SOLUTIONS

For countries with whom the United States has established investment treaties, challenges raised by the national security exception will likely be addressed during treaty negotiations. However, for countries without an investment treaty with the United States, or that are currently undergoing difficult treaty negotiations due to political tensions, such as China, foreign investors must navigate through the CFIUS's process.

Recognizing the national security risk posed by China, scholars have proposed that it would be wise for the United States to adapt a more effective strategy to protect U.S. personal data "than one-off bans on companies or where they send their data."[189] To do so, the United States should address legitimate national security risk as part of a broader initiative on comprehensive data

Ralls Corp. v. Comm. on Foreign Inv. in the U.S., 926 F. Supp. 2d 71, 88–89 (D.D.C. 2013), *rev'd and remanded*, 758 F.3d 296 (D.C. Cir. 2014).

182. McGahn II et al., *supra* note 126; *see also CFIUS Monitoring and Enforcement*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-monitoring-and-enforcement (last visited Feb. 23, 2023).

183. McGahn II et al., *supra* note 126.

184. Wang & Oguh, *supra* note 10.

185. *Id.*

186. *Id.*

187. Liu, *supra* note 62, at 361.

188. Ji Li, *Investing Near the National Security Black Hole*, 14 BERKELEY BUS. L.J. 1, 1 (2017).

189. 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.

privacy.[190] Further, a legal mechanism such as CFIUS should require greater transparency and accountability to uphold the United States' commitment to building an open economic environment that fosters economic transactions among countries.

A. GREATER TRANSPARENCY AND ACCOUNTABILITY FOR CFIUS

Without clearer insights surrounding CFIUS, interested foreign investors are forced to navigate an "opaque regulatory landscape scattered with loosely defined terms, determinations based on classified information, and decisions that offer little to no redress."[191]

One way to increase transparency would be to provide greater insight into CFIUS's advisory opinions. At the moment, CFIUS determinations are nonpublic classified information. One commentator has argued that while it is not in the U.S. government's best interest to ask CFIUS to state what national security entails, CFIUS could at least issue an advisory opinion following a determination as to why it chooses not to review a transaction.[192] Such an opinion would provide greater transparency and guidance to the business community. Further, the Committee could also provide more insights into its decisionmaking process by providing justification for a negative ruling.[193]

Comparing the statutory scheme between CFIUS and IEEPA, another commentator has argued that CFIUS could enhance its accountability safeguard analogous to the statutory mechanism of the Office of Foreign Assets Control (OFAC) under IEEPA.[194] This is because CFIUS and OFAC share a similar focus on national security, and because their governing statutes confer similar power on the Executive.[195] Similar to CFIUS, OFAC, administered by the Department of Treasury, is charged with protecting national security and may prohibit trading with or providing economic support to sanctioned individuals or persons in sanctioned countries.[196] To encourage "greater deliberation prior to taking action" and limit "OFAC's scope of allowable action," IEEPA requires the President to declare a national emergency prior to taking action as an ex ante check on OFAC.[197] Again, some have argued that CFIUS could adopt a similar mechanism by clarifying the national security definition as an ex ante safeguard to the CFIUS review process.[198]

---

190. *Id.*
191. Deeley, *supra* note 181, at 130.
192. *Id.* at 149.
193. *Id.* at 150.
194. *See generally* E. Maddy Berg, Note, *A Tale of Two Statutes: Using IEEPA's Accountability Safeguards To Inspire CFIUS Reform*, 118 COLUM. L. REV. 1763 (2018).
195. *Id.* at 1765.
196. *Id.* at 1780.
197. *Id.* at 1792.
198. *Id.* at 1793–94.

Furthermore, the IEEPA requires OFAC to transmit certain information regarding its actions and motivations to Congress even while the action is ongoing under IEEPA.[199] Requiring a greater level of congressional oversight over CFIUS may constitute another measure to ensure the confidentiality and speed of CFIUS review.[200]

B. CAN DATA-LOCALIZATION LAW BE A SOLUTION?

The central issue surrounding the ban of TikTok and foreign investment in U.S. businesses that possess significant private user data is that the use of private data by interested foreign actors may impede national security interests. This raises the question of whether it would, in fact, be more prudent for the U.S. government to regulate the use and transmission of private data rather than restricting foreign investment in the area. While certain advocates believe that divesting investment interest and control from these U.S. businesses of concern may be sufficient, cyberpolicy scholars challenge such a simplistic approach, noting that American companies can still sell data to third-party data brokers, and that those brokers could then sell the data to foreign governments.[201] The case of Cambridge Analytica exemplifies the threat that data brokers may pose to national security.[202] Governments need to develop a regulatory scheme restricting data disclosable by data brokers to further limit the sharing of private data with interested third parties. Data-localization law could be a possible alternative solution to national security review mechanisms like CFIUS review.

Data-localization law refers to "policies or mandates requiring certain data related to citizens or residents of a country—whether personal, health, business, or financial—to be physically stored on infrastructure within that country's borders."[203] For instance, under China's 2017 Cybersecurity Law and 2020 draft Personal Information Protection Law, various forms of data are required to be stored in China and undergo a government "security review" before transfer.[204] While such regulation would certainly address concerns surrounding foreign interested parties using legal means to acquire American private data that may threaten national security interests, countries like the United States are in fact pushing back against the trend toward data localization.

The idea of "data free flow with trust" was promoted by the Group of 20 and acknowledges that "cross-border flow of data, information, ideas, and knowledge generates higher productivity, greater innovation, and improved

199. *Id.* at 1794.

200. *Id.* at 1797.

201. Dymples Leong & Teo Yi-Ling, *Data Brokers: A Weak Link in National Security*, THE DIPLOMAT (Aug. 21, 2020), https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/.

202. *Id.*

203. Lindsey R. Sheppard, Erol Yayboke & Carolina G. Ramos, *The Shift Toward Data Localization*, CTR. FOR STRATEGIC & INT'L STUD. (July 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/Sheppard_TheShiftTowardDataLocalization_PullOutSection.pdf?aqf3UcmQdpPGu9cJYmrw1uaXBw3ShbrW.

204. *Id.*

sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security."[205] Scholars have observed that the United States signals its stance against data localization through international governmental bodies and bilateral and multilateral trade agreements such as the United States-Mexico-Canada Agreement, which prohibits data localization and formalizes the free flow of data between the member nations.[206] However, when it comes to China, some policymakers are inclined to enforce data-localization law. For example, on November 18, 2019, Senator Josh Hawley introduced the National Security and Personal Data Protection Act of 2019.[207] The Act, currently pending on the Committee on Commerce, Science, and Transportation, would prohibit the transfer of data to, and the storage of data within, foreign countries that threaten U.S. national security.[208] The Act further requires that China and Russia be designated as "countr[ies] of concern."[209]

It is indeed a paradox whether data-localization law could be a solution. On one hand, data-localization law may restrict the free flow of information to adverse foreign states; but on the other, localizing data may be a tool of digital authoritarianism to limit democracy, placing limits on security actors' collaboration and capabilities, and introducing risk and complexity to companies' cybersecurity operations.[210] However, compared to the current regime, where the U.S. government relies on CFIUS's expansive power to review foreign investment in American businesses that possess sensitive private data, data localization may help promote transparency and accountability for foreign investment.

CONCLUSION

In the area of foreign investment, and particularly Chinese investment in American businesses that possess sensitive private data, the U.S. government has demonstrated little self-restraint in employing national security grounds to justify its expansive power to interfere with such transactions. There is also arguably a lack of remedies from international organizations like the WTO due to the controversy surrounding the use of the national security exception clause. Development in this area supports the growing literature noting that the current international trade and investment regime can no longer support new challenges that major countries face regarding national security threats.

Against this backstop, the United States has a policy regime under CFIUS and the Commerce Department that is afforded large discretion and arguably

205. Sheppard et al., *supra* note 100, at 4.
206. *Id.* at 3.
207. National Security and Personal Data Protection Act of 2019, S. 2889, 116th Cong. (2019).
208. *Id.* § 3(a)(4).
209. *Id.* § 2(2)(A)(i)–(ii).
210. *See id.*

lacks transparency, which may hinder cross-border transactions in a booming American industry. Providing greater transparency and accountability in the national security review bureaucracy and enacting data-localization law may provide solutions to protect vital national security interests while promoting cross-border transactions.