ESSAY

NATIONAL SECURITY CREEP IN CORPORATE TRANSACTIONS

Kristen E. Eichensehr & Cathy Hwang***

National security review of corporate transactions has long been a relatively sleepy corner of regulatory policy. But as governments merge economic and national security, national security reviews are expanding in frequency and scope, causing numerous deals to be renegotiated or even blocked. This expansion of national security's impact on corporate transactions—which this Essay calls "national security creep"—raises theoretical questions in both national security and contract law and has important practical implications for dealmaking and the economy.

This Essay makes several contributions. First, it provides an updated account of the national security review process for investments, which has changed substantially in recent years with the expansion of the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS), the global diffusion of CFIUS-like processes, and U.S. moves to regulate outbound investment. Second, this Essay considers the theoretical impact of national security creep. It argues that the executive branch's increasingly broad claims about what constitutes national security may cause judges to alter long-standing deference to the executive on national security issues, with implications for deal parties, the executive, and scholars who debate whether courts should treat national security as "exceptional." It also argues that CFIUS's temporally tentacular review authority upends well-understood contract theory that

---

* Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, University of Virginia School of Law.

** Barron F. Black Research Professor of Law, University of Virginia School of Law. For helpful comments and conversations, the authors thank Kathleen Claussen, Ashley Deeks, David Fagan, Jill E. Fisch, Larry Fullerton, Jack Goldsmith, John Harrison, Michael Knoll, Ronald Lee, Michael Livermore, Paul Mahoney, Thomas Nachbar, Richard Re, Sam Rascoff, Paul Schwartz, and David Zaring, as well as participants in workshops at Columbia Law School, the Council on Foreign Relations, Georgia Tech's Internet Governance Project, George Washington University Law School, the Harvard–Yale–Stanford Junior Faculty Forum, N.Y.U. School of Law, Princeton University, Temple University Beasley School of Law, the University of Florida Levin College of Law, University of Georgia School of Law, University of Iowa College of Law, University of Minnesota Law School, University of Pennsylvania Carey Law School, and University of Virginia School of Law. Thanks to Sean Michael Blochberger, Lauren Burns, Joshua Goland, Hannah Keefer, Melissa Privette, Dev Ranjan, and Divya Vijay for excellent research assistance, and to the *Columbia Law Review* editors for their helpful suggestions and hard work in bringing the Essay to publication.

considers regulatory review to be an ex ante contract design cost. Finally, this Essay considers practical implications of national security creep and concludes with suggestions for how the executive, courts, Congress, and scholars should approach national security creep going forward.

INTRODUCTION

In the last few years, the U.S. government has ordered a Chinese company to unwind its acquisition of the dating app Grindr,[1] blocked a joint venture between a U.S. robotics company and its Chinese partner,[2] and

1. James Griffiths, Gay Dating App Grindr Is the Latest Victim of US-China Tensions, CNN Bus. (May 14, 2019), https://www.cnn.com/2019/05/14/tech/grindr-china-us-security/index.html [https://perma.cc/GL8Y-FAXR] (last updated May 15, 2019) (reporting that Chinese company Kunlun Tech, which owned 60% of Grindr, "reached an agreement with CFIUS to sell the app by June 30, 2020").

2. Paul Marquardt, Chase D. Kaniecki & Nathanael Kurcab, CFIUS Blocks Joint Venture Outside the United States, Releases 2018–2019 Data, and Goes Electric, Cleary Gottlieb: Cleary Foreign Inv. & Int'l Trade Watch (June 3, 2020), https://www.clearytradewatch.com/2020/06/cfius-blocks-joint-venture-outside-the-united-states-releases-2018-2019-data-and-goes-electronic/ [https://perma.cc/9XUV-U7LV] (noting that CFIUS blocked a robotics joint venture in China between a U.S. manufacturing company and two U.S. joint venture partners).

barred U.S. entities from investing in companies linked to China's military and surveillance industry.[3] These actions are evidence of a phenomenon this Essay calls "national security creep": the recent expansion of national security–related review and regulation of cross-border investments to allow government intervention in more transactions than ever before.

One driver of national security creep is the Committee on Foreign Investment in the United States (CFIUS)—an interagency committee in the executive branch that reviews foreign investment into the United States for national security concerns.[4] Historically, CFIUS reviewed a small number of deals a year, ordering mitigation measures in deals with obvious national security implications, such as foreign government–controlled investments in U.S. defense contractors.[5] In recent years, however, it has reviewed hundreds of transactions a year, blocked several, and, via presidential order, ordered deals to be unwound after they have closed.[6] And CFIUS's purview is only increasing, pushed along by a major congressional expansion of its jurisdiction in 2018.[7]

3. Jeanne Whalen & Ellen Nakashima, Biden Expands Trump Order by Banning U.S. Investment in Chinese Companies Linked to the Military or Surveillance Technology, Wash. Post (June 3, 2021), https://www.washingtonpost.com/technology/2021/06/03/investment-ban-chinese-surveillance-tech/ (on file with the *Columbia Law Review*).

4. The Committee on Foreign Investment in the United States (CFIUS), U.S. Dep't of the Treasury, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/6ZKF-NR4B] [hereinafter U.S. Dep't of the Treasury, CFIUS] (last visited Oct. 5, 2022).

5. David Zaring, CFIUS as a Congressional Notification Service, 83 S. Cal. L. Rev. 81, 87 (2009) (noting that, at the time of writing, "the Committee itself almost never actually prevent[ed] foreign acquisitions from going forward" and that "CFIUS ha[d] launched in-depth reviews of acquisitions in thirty-seven of the 1800-plus filings made since 1998").

6. See, e.g., Farhad Jalinous, Karalyn Mildorf, Keith Schomig, Ryan Brady & Timothy Sensenig, CFIUS 2021 Annual Report Reveals Record Filings and Continued Encouraging Trends, White & Case LLP (Aug. 5, 2022), https://www.whitecase.com/insight-alert/cfius-2021-annual-report-reveals-record-filings-and-continued-encouraging-trends [https://perma.cc/N9QZ-C8LB] (reporting on recent CFIUS filing trends and CFIUS actions on filings); see also infra notes 69–70 and accompanying text (detailing blocked transactions).

7. See infra notes 83–102 and accompanying text.

While practitioners have tracked the increase in CFIUS activity,[8] CFIUS has received little attention from legal scholars.[9] This Essay takes into account recent developments to chronicle how the reach of national security reviews is creeping outward both within and outside of the United States, leading to important consequences for both national security and corporate transactions.

While corporate transactions are subject to a variety of regulatory reviews, national security has always been special. For instance, the CFIUS review process is cloaked in secrecy.[10] *Bloomberg* recently wished "[g]ood luck" to those seeking to understand CFIUS's work, noting that CFIUS "investigations are effectively a black box."[11] As a result of CFIUS's secrecy, it can be hard for deal parties to gauge the risk that CFIUS will review or disrupt their transaction. The co-head of JPMorgan Chase's mergers and

---

8. See, e.g., 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 [https://perma.cc/UQ7E-3C84] (predicting how the Biden Administration will use the CFIUS review process); Farhad Jalinous, Karalyn Mildorf, Keith Schomig & Timothy Sensenig, CFIUS Outreach on Non-Notified Transactions: What It Means, What to Expect, and How to Successfully Navigate the Process, White & Case LLP (June 1, 2021), https://www.whitecase.com/publications/alert/cfius-outreach-non-notified-transactions-what-it-means-what-expect-and-how [https://perma.cc/V6SJ-JVMX] [hereinafter CFIUS Outreach on Non-Notified Transactions] (noting that the passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) resulted in a "significant increase in resources allocated [to CFIUS] for monitoring and enforcement and the establishment of a formal process to identify non-notified transactions" and providing information on how CFIUS reviews non-notified transactions).

9. Over the last dozen years, there appear to be three main articles that discuss national security review in the deal context in the legal academic literature. See Jon D. Michaels, The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond, 97 Va. L. Rev. 801 (2011) [hereinafter Michaels, Presidential Spinoffs]; Andrew Verstein, The Corporate Governance of National Security, 95 Wash. U. L. Rev. 775 (2018); Zaring, supra note 5. All of them predate, and thus do not account for, the recent "national security creep" that this Essay addresses. See infra note 51.

10. Because CFIUS reviews deals for national security risk, it must necessarily keep the details of many of those risks under wraps. Filings with CFIUS are confidential, and the Committee does not divulge whether particular transactions are under review, the nature of risks identified with respect to particular transactions or investors, or the contents of mitigation agreements entered into to address national security risks. See U.S. Dep't of the Treasury, CFIUS, supra note 4 (noting that "Section 721 of the Defense Production Act of 1950 . . . mandates confidentiality protections with respect to information filed with the Committee" and that "[c]onsistent with section 721, the Committee does not publicly confirm or deny that a transaction has been notified to CFIUS" (emphasis omitted)).

11. Saleha Mohsin & Daniel Flatley, All About CFIUS, the Watchdog Biden May Use to Review Musk's Ventures, Bloomberg (Oct. 21, 2022), https://www.bloomberg.com/news/articles/2022-10-21/all-about-cfius-us-watchdog-on-foreign-dealmaking-quicktake-l9ivzn5i (on file with the *Columbia Law Review*); see also John Schmidt, Ronald D. Lee & Ludovica Pizzetti, UK National Security Reviews: Insight Into Emerging Trends After First Deal Gets Blocked, Arnold & Porter Kaye Scholer LLP (Aug. 15, 2022), https://www.arnoldporter.com/en/perspectives/advisories/2022/08/uk-national-security-reviews [https://perma.cc/7L3Q-9D8L] (characterizing the U.K. investment screening process as a "black box").

acquisitions team, for instance, memorably called CFIUS "the ultimate regulatory bazooka."[12]

But while CFIUS's secrecy is not new, the recent expansion of its jurisdictional scope is. CFIUS has traditionally scrutinized deals that seemed clearly related to U.S. national security interests. For example, the first deal it reviewed, in 1987, was the proposed sale of an early Silicon Valley semiconductor company to Japan's Fujitsu at a time when the Reagan Administration considered Japan's growing semiconductor industry a threat to U.S. development of computers, robotics, and related technologies.[13] Now, however, the government's interests—and CFIUS's congressionally mandated jurisdiction—have expanded to include foreign real estate investments located near sites of national security concern,[14] and foreign investment in businesses that control or produce critical technologies, infrastructure, and data.[15] In many of these cases, foreign investment is indirect or noncontrolling—but CFIUS's tentacles still find their way in.[16] CFIUS review now captures a wide variety of deal parties, structures, activities, and policies in its attempt to protect national security, and this creeping review has significantly magnified uncertainty for corporate deal parties.[17]

But CFIUS review of investments into the United States is not the sole component of national security creep. Countries around the world—some

---

12. Kevin Granville, CFIUS, Powerful and Unseen, Is a Gatekeeper on Major Deals, N.Y. Times (Mar. 5, 2018), https://www.nytimes.com/2018/03/05/business/what-is-cfius.html (on file with the *Columbia Law Review*).

13. Fairchild Semiconductor called off the transaction in 1987, "reportedly 'bowing to intense pressure from Reagan Administration officials.'" Grace Maral Burnett, Analysis: Semiconductors Made CFIUS, Bloomberg L. (June 12, 2020), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-semiconductors-made-cfius [https://perma.cc/GN6Z-HZJX] (quoting David E. Sanger, Japanese Purchase of Chipmaker Canceled After Objections in U.S., N.Y. Times (Mar. 17, 1987), https://www.nytimes.com/1987/03/17/business/japanese-purchase-of-chip-maker-canceled-after-objections-in-us.html (on file with the *Columbia Law Review*)) (describing the semiconductor industry as one that has always particularly interested national security regulators); see also Chris Miller, A Semiconducted Trade War, Foreign Pol'y (July 1, 2019), https://foreignpolicy.com/2019/07/01/a-semiconducted-trade-war/ [https://perma.cc/6KB6-9DF2] (describing the U.S.–Japan trade war over semiconductors in the 1980s).

14. Gordon F. Peery, Commercial Leases and Other Real Estate Transactions Are Subject to National Security Review, Law.com (July 8, 2021), https://www.law.com/2021/07/08/commercial-leases-and-other-real-estate-transactions-are-subject-to-national-security-review/ (on file with the *Columbia Law Review*) (noting that, in some cases, leasing or purchasing property that is close to national security interests may trigger CFIUS review).

15. James K. Jackson, Cong. Rsch. Serv., RL33388, The Committee on Foreign Investment in the United States (CFIUS) 2 (2020), https://sgp.fas.org/crs/natsec/RL33388.pdf [https://perma.cc/G576-QZZ4] (noting that FIRRMA allows CFIUS "to review any noncontrolling investment in U.S. businesses involved in critical technology, critical infrastructure, or collecting sensitive data on U.S. citizens").

16. See infra notes 86–89 and accompanying text.

17. See infra section II.B.

encouraged by the United States—are establishing their own CFIUS-like processes to screen inbound foreign investment for national security concerns.[18] And creep is not even limited to regulating inbound investment. Both the executive branch and Congress are becoming increasingly interested in regulating *outbound* investment on national security grounds. In 2021, the Biden Administration doubled down on regulations issued at the end of the Trump Administration to prohibit U.S. persons from investing in companies linked to China's military.[19] National Security Advisor Jake Sullivan warned that the Biden Administration is "looking at the impact of outbound U.S. investment flows that could . . . enhance the technological capacity of our competitors in ways that harm our national security,"[20] and Congress is actively considering establishing a CFIUS-like committee to review outbound investments in countries of concern.[21]

In addition to identifying and describing the phenomenon of national security creep, this Essay makes several theoretical contributions to literatures in national security law, corporate law, and contract law.

The expanding ambit of national security reviews ties into existing debates about judicial deference to the executive branch on foreign relations and national security.[22] As the political branches engage in ever-broader actions in the name of national security, the role of the courts as a potential overseer or check is an obvious consideration. Judges tend to defer to the executive on national security issues, but national security creep is already leading to more and somewhat different cases, challenging the traditional deference paradigm.[23] Judges could continue to defer to the executive, expanding the scope of their deference to match

18. See infra section I.B.2.

19. See infra notes 149–164 and accompanying text.

20. Press Release, The White House, Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit (July 13, 2021), https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit/ [https://perma.cc/UNY8-APRA].

21. See infra notes 165–174 and accompanying text.

22. Judicial deference to the executive branch in national security and foreign affairs–related cases has sparked numerous law review articles describing and critiquing the amount of, and rationales for, such deference. See, e.g., Curtis A. Bradley, *Chevron* Deference and Foreign Affairs, 86 Va. L. Rev. 549 (2000) [hereinafter Bradley, *Chevron* Deference and Foreign Affairs]; Robert M. Chesney, National Security Fact Deference, 95 Va. L. Rev. 1361 (2009); Ashley S. Deeks, The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference, 82 Fordham L. Rev. 827 (2013); Kristen E. Eichensehr, Courts, Congress, and the Conduct of Foreign Relations, 85 U. Chi. L. Rev. 609 (2018); Kristen E. Eichensehr, Foreign Sovereigns as Friends of the Court, 102 Va. L. Rev. 289 (2016) [hereinafter Eichensehr, Foreign Sovereigns as Friends of the Court]; Derek Jinks & Neal Kumar Katyal, Disregarding Foreign Relations Law, 116 Yale L.J. 1230 (2007); Deborah N. Pearlstein, After Deference: Formalizing the Judicial Power for Foreign Relations Law, 159 U. Pa. L. Rev. 783 (2011); Eric A. Posner & Cass R. Sunstein, *Chevron*izing Foreign Relations Law, 116 Yale L.J. 1170 (2007).

23. See infra section II.A.1.

the scope of the national security claims. But there is some early evidence that judges might be shifting their approach either to constrict deference across the board or to bifurcate deference based on whether the executive is addressing a "traditional" national security concern or an economically focused one like those on which this Essay focuses.[24] Such adjustments to judicial deference will affect the executive and regulated parties and have the potential to complicate scholarly debates about whether national security and foreign relations are subject to exceptional rules or are instead being "normalized" toward a domestic law baseline.[25]

National security creep also muddies the conventional understanding of how to manage contracting costs in corporate transactions. Contract theorists have long made a distinction between the ex ante costs of contracting, such as the costs associated with negotiating and drafting the contract, and the ex post costs, which include litigation costs and the uncertainty of the deal outcome.[26] More investment ex ante should reduce litigation probability and complexity, thereby decreasing ex post costs.[27] The nature of national security review weakens the link between the two: As many deal parties have learned, for instance, it is hard to manage ex post costs through ex ante investment when CFIUS intervention is so uncertain.

Beyond these theoretical points, this Essay's descriptive account of national security creep also raises a number of practical implications that warrant further exploration.

From the national security side, an important question is whether global diffusion of CFIUS-like processes might stoke nationalism and blowback in investment reviews. Will the CFIUS-like processes the U.S. government has encouraged allies to establish be turned against U.S. investors going forward? From the corporate side, national security review

---

24. See infra section II.A.1.

25. See infra section II.A.2.

26. See, e.g., Richard A. Posner, The Law and Economics of Contract Interpretation, 83 Tex. L. Rev. 1581, 1583 (2005) (defining the cost of a contract as the ex ante negotiating and drafting costs, plus the probability of litigation multiplied by the sum of the parties' litigation costs, the judiciary's litigation costs, and judicial error costs).

27. See, e.g., Albert Choi & George Triantis, Strategic Vagueness in Contract Design: The Case of Corporate Acquisitions, 119 Yale L.J. 848, 852 (2010) (arguing that parties can use vague contract provisions efficiently—for example, material adverse change clauses in acquisition agreements may remain vague because they are rarely litigated); Cathy Hwang, Unbundled Bargains: Multi-Agreement Dealmaking in Complex Mergers and Acquisitions, 164 U. Pa. L. Rev. 1403, 1419 (2016) [hereinafter Hwang, Unbundled Bargains] (discussing how modularizing a contract ex ante can reduce litigation costs ex post); Robert E. Scott & George G. Triantis, Anticipating Litigation in Contract Design, 115 Yale L.J. 814, 818 (2006) (examining the efficiency of investment in the design and enforcement phase of the contracting process and arguing that parties can lower overall contracting costs by using vague contract terms ex ante and shifting investment to the ex post enforcement phase); Robert E. Scott & George G. Triantis, Incomplete Contracts and the Theory of Contract Design, 56 Case W. Rsrv. L. Rev. 187, 189 (2005) (considering the role of litigation in motivating contract design).

increases uncertainty in dealmaking. Will deal parties' attempts to dodge regulatory scrutiny also decrease the amount of information available to investors? And will national security creep reduce overall deal volume?

The remainder of this Essay proceeds as follows. Part I offers a descriptive account of national security creep in corporate deals, situating U.S. government moves to merge economic and national security in a broader context and focusing on three recent developments: the expansion of CFIUS's jurisdiction, the diffusion of CFIUS-like processes around the world, and stepped-up U.S. regulation of outbound investment. Part II discusses theoretical implications of national security creep for national security law and for contract law, and Part III identifies additional practical implications for further research. While the Essay sounds some notes of caution about national security creep, the Conclusion explains why we do not here take a stronger normative position on the desirability (or not) of expanded national security review of investments, and it closes by discussing how we think executive branch officials, judges, legislators, deal parties, and scholars should approach national security creep going forward.

I. NATIONAL SECURITY CREEP

Security in general and national security in particular are notoriously indeterminate concepts.[28] National security is contested within and among states, and the boundaries of what counts as security are expanding rapidly. To take just one example, the 2022 *Annual Threat Assessment of the U.S. Intelligence Community*, prepared by the Office of the Director of National Intelligence (DNI), includes sections on China, Russia, Iran, North Korea, and global terrorism, but it also addresses health security, "climate change and environmental degradation," "innovative use of new technology," and migration.[29] The U.S. understanding of national security threats has

28. For a helpful attempt to unpack and systematize understandings of security, see J. Benton Heath, Making Sense of Security, 116 Am. J. Int'l L. 289, 291 (2022) [hereinafter Heath, Making Sense of Security] ("Security . . . is a deeply indeterminate concept, whose power derives not only from its association with particular issues or threats, but from the way that it combines fundamental ambiguity with a sense of heightened urgency.").

29. Off. of the Dir. of Nat'l Intel., Annual Threat Assessment of the U.S. Intelligence Community 3 (2022), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf [https://perma.cc/WP5J-V2UM]; see also The White House, National Security Strategy 6 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf [https://perma.cc/36ZZ-WD9V] (describing "climate change, food insecurity, [and] communicable diseases," among other things as "not marginal issues that are secondary to geopolitics" but rather "at the very core of national and international security"); Sir Jeremy Fleming, Dir., Gov't Commc'ns Headquarters, If China Is the Question, What Is the Answer? (Oct. 11, 2022) (UK), https://rusi.org/events/open-to-all/rusi-annual-security-lecture-2022-sir-jeremy-fleming-director-gchq (transcript on file with the *Columbia Law Review*) (explaining that "we are constantly re-thinking what we mean when we say 'national security'" and that "technology, security, economics and statecraft are entangled and mutually dependent").

clearly moved far beyond traditional state-to-state conflict and even the post-9/11 focus on transnational terrorism.[30] Expanding national security's scope, however, has only exacerbated the concept's indeterminacy, making it hard to define what is—and is not—national security.[31]

This Essay focuses on one category of national security–based decisions: restrictions on inbound and outbound investment. The growth in deals subject to national security reviews—a phenomenon this Essay calls "national security creep"—provides a window into broader questions about the theoretical and practical implications of expanding the understanding of national security. Investment restrictions are tied most directly to one particular feature of national security's expansion, namely moves by states, including the United States, to merge economic security and national security. Section I.A discusses this conflation of economic and national security, which has set the stage for existing national security review of investments to spread beyond their historical scope. Section I.B then discusses several developments as concrete examples of creep: the expansion of CFIUS's jurisdiction, adoption of CFIUS-like review processes by countries around the world, and moves to restrict outbound investments from the United States to China in particular, and possibly more broadly, as Congress considers establishing an "outbound CFIUS" process.

A. *The Conflation of Economic and National Security*

The economic turn in national security has become explicit in U.S. policy. The Trump Administration pushed the mantra that "[e]conomic security is national security" in its 2017 *National Security Strategy*[32] and cited national security to justify all sorts of trade- and investment-related actions.[33] The Biden Administration's *Interim National Security Strategic*

30. Cf. Harlan Grant Cohen, Nations and Markets, 23 J. Int'l Econ. L. 793, 806 (2020) ("Today, no one blinks when data and cyber security, terrorism, economic crisis, drug and human trafficking, infectious diseases, and even climate change are described as national security concerns.").

31. Cf. id. at 807 (noting that the expansion runs a risk that "national security collapses upon itself, becoming synonymous with national advantage or disadvantage"); Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, Toward a Geoeconomic Order in International Trade and Investment, 22 J. Int'l Econ. L. 655, 665 (2019) [hereinafter Roberts et al., Toward a Geoeconomic Order] (arguing that "[t]reating economic security as national security may . . . create a permanent state of exception justifying broad protection/protectionist measures" and that "mixing notions of competition, conflict, and rivalry across economic, political, and security realms" makes it "hard to know when a threat might be understood as starting or finishing").

32. The White House, National Security Strategy of the United States of America 17 (2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [https://perma.cc/H8PU-3C7Q].

33. See, e.g., Ana Swanson & Paul Mozur, Trump Mixes Economic and National Security, Plunging the U.S. Into Multiple Fights, N.Y. Times (June 8, 2019), https://www.nytimes.com/2019/06/08/business/trump-economy-national-security.html (on file with the *Columbia*

Guidance reiterated the marriage of economic and national security, asserting that "our policies must reflect a basic truth: in today's world, economic security is national security."[34]

These assertions are consistent with broader trends that scholars have identified with respect to international trade and economic law more generally.

Anthea Roberts, Henrique Choer Moraes, and Victor Ferguson have described a shift from the post–Cold War "old international economic world order" where "national security—or, at least, U.S. national security—and international trade and investment appeared to operate on relatively independent tracks,"[35] to a "new geoeconomic world order, characterized by great power rivalry between the United States and China and the clear use of economic tools to achieve strategic goals."[36] They argue that under the old order, security

> existed on the margins . . . as a premise for the order (in the sense of being a justification for states entering into trade and investment agreements), and an exception to the order (in the sense that national security was one of a handful of exceptions permitted to trade and investment rules), but not as the rule that governed the regime's core.[37]

The United States began to shift to a new paradigm around 2008, they argue, and clearly changed strategy in 2017 and 2018, such that "[s]ecurity moved from being the premise and a relatively unused exception . . . to becoming a broadly invoked exception with the capacity to swallow the rule."[38]

J. Benton Heath and Kathleen Claussen have similarly highlighted states' expanding conceptions of national security in the international

---

Law Review) (chronicling Trump Administration invocations of national security for economic actions).

34. The White House, Interim National Security Strategic Guidance 15 (2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf [https://perma.cc/7YNV-MCTF]; see also id. at 22 ("[T]raditional distinctions between foreign and domestic policy—and among national security, economic security, health security, and environmental security—are less meaningful than ever before . . . .").

35. Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, The Geoeconomic World Order, Lawfare (Nov. 19, 2018), https://www.lawfareblog.com/geoeconomic-world-order [https://perma.cc/4QUR-WL4P].

36. Id.; see also Roberts et al., Toward a Geoeconomic Order, supra note 31, at 657 (describing the "Geoeconomic Order").

37. Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, Geoeconomics: The Variable Relationship Between Economics and Security, Lawfare (Nov. 27, 2018), https://www.lawfareblog.com/geoeconomics-variable-relationship-between-economics-and-security [https://perma.cc/32XJ-ARRR].

38. Id.

trade arena.[39] Expansive claims by states pursuant to national security exceptions in trade agreements have put pressure on the international trade system, making it "increasingly difficult today to place such [national security] measures entirely outside of a legal order, lest the exception entirely swallow the rule."[40]

The question of what exactly is beyond the reach of national security claims arises in the investment screening sphere as well. Deducing the scope of national security from U.S. government actions makes clear that dating apps, for instance, are now national security matters. In 2019, CFIUS ordered the unwinding of a deal in which Beijing-based Kunlun Technology had purchased a 60% stake in American dating app Grindr.[41] Although CFIUS does not publicly explain its decisions, reports speculated that the U.S. government's action rested on concerns that the Chinese government could access sensitive personal data shared via the app, especially information pertaining to U.S. government officials.[42] Social media apps implicate national security too: The Trump Administration sought to ban TikTok and other Chinese-owned apps due to national security worries,[43] and concerns about TikTok in particular have continued in the Biden Administration.[44] FBI Director Christopher Wray testified to Congress in November 2022 that TikTok poses national security risks due to "the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm,

39. Kathleen Claussen, Trade's Security Exceptionalism, 72 Stan. L. Rev. 1097, 1106 & n.20 (2020) (noting the Trump Administration's expansion of claims of national security with respect to trade law and other areas); J. Benton Heath, The New National Security Challenge to the Economic Order, 129 Yale L.J. 1020, 1034 (2020) [hereinafter Heath, The New National Security Challenge] (describing "the collision between economic rules and the new national security" and how it will "challenge the ordinary operation of trade and investment rules").

40. Heath, The New National Security Challenge, supra note 39, at 1080–81; see also Heath, Making Sense of Security, supra note 28, at 328–31 (discussing recent World Trade Organization panel decisions about national security exceptions).

41. Griffiths, supra note 1.

42. See id.

43. Kristen Eichensehr, United States Pursues Regulatory Actions Against TikTok and WeChat Over Data Security Concerns, *in* Contemporary Practice of the United States Relating to International Law, 115 Am. J. Int'l L. 124, 124–25 (2021) [hereinafter Eichensehr, Regulatory Actions Against TikTok]; Jeanne Whalen & Ellen Nakashima, Biden Revokes Trump's TikTok and WeChat Bans, But Sets Up a Security Review of Foreign-Owned Apps, Wash. Post (June 9, 2021), https://www.washingtonpost.com/technology/2021/06/09/tiktok-ban-revoked-biden/ (on file with the *Columbia Law Review*) [hereinafter Whalen & Nakashima, Biden Revokes Bans] (reporting that divestment negotiations between CFIUS and TikTok's Chinese parent company are continuing in the Biden Administration).

44. See, e.g., Bobby Allyn, TikTok Says It's Putting New Limits on Chinese Workers' Access to U.S. User Data, NPR (July 1, 2022), https://www.npr.org/2022/07/01/1109467942/tiktok-china-data-privacy [https://perma.cc/YP7D-3J8T] (discussing negotiations between TikTok and the Biden Administration over safeguards for U.S. user data in response to security concerns from U.S. officials).

which could be used for influence operations . . . , or to control software on millions of devices."[45] Negotiations between TikTok and CFIUS about measures to mitigate national security risks are reportedly ongoing.[46]

Secretary of State Antony Blinken has signaled that the United States is "sharpening" its "tools to safeguard [its] technological competitiveness," including through "sharper investment screening measures to defend companies and countries against Beijing's efforts to gain access to sensitive technologies, data, or critical infrastructure."[47] The following section takes a deep dive into how new understandings about national security manifest in investment screening mechanisms.

B. *The Expanding Reach of National Security Reviews of Investments*

The conflation of economic and national security has set the stage for governments to turn ever more frequently to national security–driven laws and regulations on commerce. Concerns about cross-border technology and data flows in particular have prompted U.S. administrations to deploy a variety of regulatory tools, like CFIUS reviews, economic sanctions, and export controls,[48] and to use existing statutory authorities, like the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act (NEA), to address national security threats.[49]

---

45. Rachel Treisman, The FBI Alleges TikTok Poses National Security Concerns, NPR (Nov. 17, 2022), https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china [https://perma.cc/CH77-45EC] (quoting Wray).

46. See id. (discussing negotiations between TikTok and CFIUS).

47. Antony J. Blinken, Sec'y of State, Address at The George Washington University: The Administration's Approach to the People's Republic of China (May 26, 2022), https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/ [https://perma.cc/9Y53-67BQ]; see also Tom C.W. Lin, Business Warfare, 63 B.C. L. Rev. 1, 40 (2022) ("[T]he United States in recent years has taken a more aggressive view on the links between national security and business interests, particularly when it involves foreign investments.").

48. See Export Administration Regulations (EAR), Bureau of Indus. & Sec., U.S. Dep't of Com., https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear [https://perma.cc/5HED-XKW7] (last visited Oct. 5, 2022) (collecting export control regulations); Learn About Export Regulations, Directorate of Def. Trade Controls, U.S. Dep't of State, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=8249bf04dbc7bf0044f9ff621f96197d [https://perma.cc/JFV7-MHNY] (last visited Oct. 8, 2022) (providing information on export of defense trade items); Sanctions Programs and Country Information, U.S. Dep't of the Treasury, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information [https://perma.cc/B547-SSJ8] (last visited Oct. 5, 2022) (listing sanctions programs).

49. See, e.g., Ellen Nakashima & Aaron Schaffer, Biden Administration Places Top Chinese Military Institute on Export Blacklist Over Its Use of Surveillance, 'Brain-Control' Technology, Wash. Post (Dec. 16, 2021), https://www.washingtonpost.com/business/2021/12/16/china-entity-list-military-institute-added/ (on file with the *Columbia Law Review*) (describing recent additions of Chinese entities to the Commerce Department's "Entity List" as part of an effort to prevent transfer of technology to entities that harm U.S. national security).

Rather than attempt to address all economic regulations related to national security, this Essay zeroes in on national security reviews of investments.[50] Because these regimes can block pending transactions and unwind closed deals, they are among the most disruptive national security–related regulatory regimes for companies. The nature and extent of the disruption they can occasion sharpens the theoretical and practical implications that follow in subsequent Parts. In particular, this section addresses three major recent developments with respect to investment reviews that contribute to national security creep: the expansion of the scope of CFIUS's review, the diffusion of CFIUS-like processes to other countries, and new regulations that restrict outbound transactions.

---

50. Another national security–focused regulatory regime that shares some similarities with the ones on which we focus is the Federal Communications Commission's (FCC) "Team Telecom" process for screening telecommunications license applications for national security concerns. Since the late 1990s, as part of its assessment of whether license applications raise "national security, law enforcement, foreign policy, or trade policy concerns," the FCC has informally referred applications to "the Departments of Defense, Homeland Security, and Justice (informally known as 'Team Telecom')." Farhad Jalinous & Ryan Brady, Team Telecom Two-Year Anniversary, White & Case LLP (Apr. 25, 2022), https://www.whitecase.com/insight-alert/team-telecom-two-year-anniversary [https://perma.cc/WPQ5-E7JY]. In 2020, the White House and FCC formalized the Team Telecom process. Executive Order 13,913 established an interagency "Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," made up of the Secretary of Defense, Attorney General, and Secretary of Homeland Security, supported by advisors from other departments, including the Secretaries of State and Treasury. Exec. Order No. 13,913, 85 Fed. Reg. 19,643, 19,643–44 (Apr. 8, 2020) (codified at 3 C.F.R. 324 (2021)). The Committee "assist[s] the FCC in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector[,]" and it can advise the FCC to grant licenses or transfers of licenses pursuant to mitigation agreements to address national security or law enforcement risks or to deny applications altogether. Id. at 19,644–45. The order also established specific timelines for the Committee's review of referred applications. Id. at 19,645–46. In September 2020, the FCC adopted rules formalizing the Team Telecom review process, including incorporating the timeframes and role of the Committee. See Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, 35 FCC Rcd. No. 20-133 (Sept. 30, 2020), https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf [https://perma.cc/7Q8X-7P69]. The FCC refers to Team Telecom applications "to provide international telecommunications service or submarine landing licenses . . . if an applicant has a 10% or greater direct or indirect foreign investment" as well as "[a]pplications to exceed the FCC's statutory foreign ownership benchmarks . . . ." FCC Standardizes and Formalizes "Team Telecom" Review, Sidley Austin LLP (Jan. 27, 2021), https://www.sidley.com/en/insights/newsupdates/2021/01/fcc-standardizes-and-formalizes-team-telecom-review [https://perma.cc/JW5U-XK2J]. The Team Telecom process shares some similarities with the CFIUS process, and a single transaction can be subject to review via both processes. 35 FCC Rcd. No. 20-133, at 15–16. As with CFIUS, a number of the FCC's recent application denials and license revocations have focused on national security concerns posed by Chinese entities. See Jalinous & Brady, supra. Although the FCC and Team Telecom's authority is limited to telecommunications issues, their authority is broader than CFIUS's in other ways. In particular, the FCC can review and revoke licenses it previously granted, whereas CFIUS generally does not reopen review of previously cleared transactions. Id.

1. *CFIUS's Increasing Scope.* — For several decades, CFIUS has reviewed inbound investment into the United States for national security concerns. While a few previous scholarly articles have discussed aspects of CFIUS review, the scope of the Committee's authority has increased dramatically in recent years, so much so as to be nearly unrecognizable from earlier accounts.[51] This section provides an in-depth account of CFIUS's process and scope as it currently operates.

a. *The CFIUS Process.* — CFIUS is an interagency committee chaired by the Secretary of the Treasury and includes representatives from the Departments of Justice, Homeland Security, Commerce, Defense, State, and Energy, as well as the Office of the U.S. Trade Representative and the Office of Science and Technology Policy.[52] The Director of National Intelligence and the Secretary of Labor serve as ex officio nonvoting members of the Committee.[53] In its current structure, CFIUS reviews

---

51. Three major articles in the last decade and a half have addressed national security reviews. See supra note 9. First, David Zaring's 2009 article made the novel argument that CFIUS functions primarily as a "congressional notification service." Zaring, supra note 5, at 90–98. But when Zaring wrote, CFIUS was far less active than it is today and, as Zaring noted, "almost never actually prevent[ed] foreign acquisitions from going forward." Id. at 87. That is no longer the case. Second, Jon Michaels's more recent 2011 article focuses on CFIUS as an example of the delegation of presidential power, but Michaels discusses the Committee in the service of the article's primary purpose of challenging the dominant scholarly view of the President as power-aggrandizing through examples of institutional design. See Michaels, Presidential Spinoffs, supra note 9, at 807–08. The third article on national security review of deals is also the one that deals with CFIUS most tangentially. Andrew Verstein's 2017 article mentions CFIUS, but it focuses on government intervention in defense companies operated under foreign ownership, control, or influence (FOCI). Verstein, supra note 9, at 792–805. As Verstein notes, under certain circumstances, such as when companies operating under FOCI are counterparties to defense contracts, the same factors that trigger FOCI review also trigger CFIUS review and similar mitigation measures. See id. at 795.

A major federal court case, Ralls Corp. v. Committee on Foreign Investment in the United States, 758 F.3d 296 (D.C. Cir. 2014), discussed infra notes 204–213 and accompanying text, also prompted a small bumper crop of student notes. See, e.g., 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 (2015); Christopher M. Fitzpatrick, Note, Where *Ralls* Went Wrong: CFIUS, the Courts, and the Balance of Liberty and Security, 101 Cornell L. Rev. 1087 (2016); Chang Liu, Note, *Ralls v. CFIUS*: The Long Time Coming Judicial Protection of Foreign Investors' Constitutional Rights Against Government and President's National Security Review, 15 J. Int'l Bus. & L. 361 (2016).

Perhaps the most important feature to note about all of these pieces is that they predate the 2018 expansion of CFIUS jurisdiction, implemented by regulation in 2020, to say nothing of the recent restrictions on outbound investment and global developments with respect to investment screening—the key ingredients this Essay identifies as evidence of national security creep.

52. U.S. Dep't of the Treasury, CFIUS Overview, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview [https://perma.cc/2Z7D-35RB] [hereinafter U.S. Dep't of the Treasury, CFIUS Overview] (last visited Oct. 5, 2022).

53. Id.

voluntary and some mandatory filings by parties to transactions that may pose national security concerns.[54]

CFIUS screens transactions using a multistep process.[55] In practice, deal parties often begin the process with a "step zero" in which they informally consult CFIUS before filing formally.[56] The official CFIUS process begins when transaction parties file either a short-form declaration or a formal written notice.[57] The filing of a written notice (whether done initially or upon CFIUS's request after the filing of a short-form declaration) triggers a forty-five-day review period during which CFIUS conducts a risk assessment to determine whether the transaction threatens to impair U.S. national security.[58] The risk assessment considers: (1) the "threat" posed by the transaction, "which is a function of the intent and capability of a foreign person to take action to impair the national security of the United States"; (2) "vulnerabilities," described as "the extent to which the nature of the U.S. business presents susceptibility to impairment of national security"; and (3) the "consequences to national security," namely, "the potential effects on national security that could reasonably result from the exploitation of the vulnerabilities by the threat actor."[59] If the national security review identifies risks that need to be resolved or if the transaction involves a foreign person controlled by a foreign government, CFIUS initiates a forty-five-day national security investigation (subject to a possible fifteen-day extension).[60]

To address identified national security risks, CFIUS may negotiate with transaction parties and conclude agreements to mitigate risks.[61] Such mitigation agreements can include a variety of requirements, like barring or limiting the sharing of intellectual property; limiting access to particular technology or customer information to authorized persons; requiring that "only U.S. citizens handle certain products and services"; "ensuring that certain activities and products are located only in the United States"; excluding "certain sensitive assets from the transaction"; and requiring the establishment of a "Corporate Security Committee and other mechanisms to ensure compliance with all required actions, including the appointment

54. As discussed below, the 2018 FIRRMA legislation altered the review process to require some mandatory filings. See infra notes 90–93 and accompanying text.

55. See 31 C.F.R. pt. 800 (2021).

56. See Jackson, supra note 15, at 15–16 (discussing the informal consultation process).

57. See id. at 16; U.S. Dep't of the Treasury, CFIUS Overview, supra note 52.

58. 31 C.F.R. §§ 800.102, 800.501–.506.

59. Id. § 800.102.

60. Id. §§ 800.505–.508; Jackson, supra note 15, at 20.

61. See Michaels, Presidential Spinoffs, supra note 9, at 825–27 (discussing CFIUS's negotiation of mitigation agreements and noting that the Committee's influence on transaction parties is substantial, as evidenced by the number of proposed transactions that are withdrawn to avoid a formal presidential decision to block them); Zaring, supra note 5, at 106–10 (discussing CFIUS's influence, including through mitigation agreements, on transaction parties beyond formal blocking of deals); see also Jackson, supra note 15, at 20.

of a U.S. Government–approved security officer and/or member of the board of directors and requirements for security policies, annual reports, and independent audits."[62] In 2020, approximately 12% of notices filed with CFIUS resulted in mitigation agreements, and for each, a CFIUS agency monitors ongoing compliance.[63]

If, at the end of the investigation, CFIUS determines that national security risks remain, it may recommend to the President that he block the transaction.[64] The President has fifteen days to determine whether to act.[65] The CFIUS statute empowers the President to "suspend or prohibit any covered transaction that threatens to impair the national security of the United States" if he finds that "there is credible evidence . . . to believe that a foreign person that would acquire an interest in a United States business or its assets as a result of the covered transaction might take action that threatens to impair the national security" and that "provisions of law, other than this section [50 U.S.C. § 4565] and the International Emergency Economic Powers Act, do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter before the President."[66]

Congress provided a nonexhaustive list of factors the President may consider in determining whether to prohibit a transaction, including the ability of domestic industries to meet national defense requirements, effects on U.S. technological leadership, and national security effects on critical infrastructure and technologies.[67] The statute significantly limits judicial review of presidential action, specifying that the President's actions to suspend or block a transaction and findings with respect to the

---

62. Comm. on Foreign Inv. in the U.S., Annual Report to Congress 40–41 (2021), https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2020.pdf [https://perma.cc/C7W5-HWLZ] [hereinafter CFIUS 2020 Report] (reporting on the calendar year 2020); see also Zaring, supra note 5, at 109 (describing mitigation agreements imposed on Lenovo, a Chinese company, when it purchased IBM's personal computer business and on a "state-owned Singaporean telecommunications company").

63. CFIUS 2020 Report, supra note 62, at 40; see also Zaring, supra note 5, at 110 ("[I]t is in the use of mitigation agreements that CFIUS does much of its regulating."). In October 2022, CFIUS issued its first "Enforcement and Penalty Guidelines" to provide details on how the Committee determines that a company has committed a violation (for example, by contravening a mitigation agreement) and on aggravating and mitigating factors CFIUS considers in determining penalties. See Memorandum from Paul M. Rosen, Asst. Sec'y of the Treasury for Inv. Sec., to the Comm. on Foreign Inv. in the U.S. (Oct. 20, 2022), https://home.treasury.gov/system/files/206/CFIUS-Enforcement-and-Penalty-Guidelines.pdf [https://perma.cc/8APM-VUS4]; see also David McCabe, U.S. Details How It Plans to Police Foreign Firms, N.Y. Times (Oct. 20, 2022), https://www.nytimes.com/2022/10/20/technology/us-foreign-firms.html (on file with the *Columbia Law Review*) (describing the Guidelines).

64. 31 C.F.R. § 800.508; Jackson, supra note 15, at 21–22.

65. 50 U.S.C. § 4565(d)(2) (Supp. III 2021).

66. Id. § 4565(d)(2), (4).

67. Id. § 4565(f).

existence of a threat to national security are not subject to judicial review.[68] To date, Presidents have blocked seven transactions,[69] including ordering ByteDance, the parent company of TikTok, to divest itself of Musical.ly.[70]

Although President Ford initially established CFIUS via executive order in 1975,[71] Congress has codified and repeatedly expanded the authority of the President and CFIUS to review and block transactions on national security grounds.[72] In 1988, Congress codified and expanded the executive branch's authorities by passing the Exon–Florio amendment to the Defense Production Act, which granted the President authority to block transactions that threaten to impair U.S. national security.[73] The Treasury Department regulations implementing Exon–Florio created a system whereby parties to a transaction voluntarily notified CFIUS, and CFIUS member agencies could also provide notices to the Committee.[74]

CFIUS's authority expanded again in the mid-2000s, based on both presidential and congressional action. In 2006, CFIUS allowed the purchase of commercial operations in six U.S. ports by Dubai Ports World—a foreign government–owned entity—prompting public and congressional outcry.[75] Although the criticism eventually prompted Dubai Ports World to sell the U.S. port operations to a U.S. company,[76] the controversy spurred the executive branch to assert authority to monitor transactions for security concerns on an ongoing basis. Prior to 2006, "CFIUS reviews and investigations were portrayed and considered to be final," a system that encouraged companies "to subject themselves voluntarily to a CFIUS review, because they believed that once an investment transaction

---

68. Id. § 4565(e)(1). The statute also specifies that civil actions "challenging an action or finding" pursuant to the CFIUS statute "may be brought only" in the D.C. Circuit, id. § 4565(e)(2), which has allowed for limited judicial review in certain circumstances, see infra notes 204–213 and accompanying text (discussing the *Ralls* case).

69. Jackson, supra note 15, at 21 (listing five blocked transactions); see also Order of August 14, 2020: Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 19, 2020) (codified at 3 C.F.R. 606 (2021)); Order of March 6, 2020: Regarding the Acquisition of StayNTouch, Inc. by Beijing Shiji Information Technology Co., Ltd., 85 Fed. Reg. 13,719 (Mar. 10, 2020) (codified at 3 C.F.R. 532 (2021)).

70. Eichensehr, Regulatory Actions Against TikTok, supra note 43, at 129; Whalen & Nakashima, Biden Revokes Ban, supra note 43; see also Treisman, supra note 45 (discussing ongoing negotiations between TikTok and CFIUS).

71. Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975) (codified at 3 C.F.R. 159 (1976)).

72. See, e.g., Zaring, supra note 5, at 91–97 (tracing the evolution of CFIUS through 2009).

73. Jackson, supra note 15, at 7–8. Congress intended the Exon–Florio provision "to strengthen the President's hand in conducting foreign investment policy, while limiting its own role as a means of emphasizing that, as much as possible, the commercial nature of investment transactions should be free from political considerations" and that the United States remains open to foreign investment. Id. at 8.

74. Id. at 8.

75. Id. at 4–5; Michaels, Presidential Spinoffs, supra note 9, at 817–18.

76. Jackson, supra note 15, at 4.

was scrutinized and approved by the members of CFIUS the firms could be assured that the investment transaction would be exempt from any future reviews or actions."[77] However, in approving France-based Alcatel SA's acquisition of Lucent Technologies, Inc., in December 2006, CFIUS required Alcatel–Lucent to agree to a "Special Security Arrangement, or SSA, that restricts Alcatel's access to sensitive work done by Lucent's research arm, Bell Labs, and the communications infrastructure in the United States."[78] This and other SSAs "allow[] CFIUS to reopen a review of a transaction and to overturn its approval at any time if CFIUS believed the companies 'materially fail to comply' with the terms of the arrangement."[79] From this point forward, CFIUS reviews became temporally tentacular, stretching beyond a single transaction approval and potentially subjecting both transactions that are approved *and* those not filed with CFIUS to post-closing review and governmental action.[80]

The Dubai Ports World controversy also spurred Congress to codify CFIUS's authority. Whereas the Exon–Florio provision codified presidential authorities, the Foreign Investment and National Security Act of 2007 (FINSA) established statutory authority for CFIUS itself.[81] Among other changes, FINSA expanded CFIUS's membership to include the Director of National Intelligence, allowed the President to consider additional factors in determining whether a transaction threatens to impair national security, and increased congressional oversight through reporting requirements and a requirement that CFIUS member agencies certify to Congress that transactions have no unresolved national security issues.[82]

b. *Changes Since 2018*. — CFIUS's authorities remained stable from 2007 until the summer of 2018 when concerns largely about Chinese investment into the United States prompted Congress to again expand CFIUS's powers in the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[83] While reaffirming the traditional policy of open investment into the United States, Congress asserted that "the national security landscape has shifted in recent years, and so has the nature of the investments that pose the greatest potential risk to national security."[84]

---

77. Id. at 9–10.

78. Id. at 9.

79. Id.

80. Cf. id. at 10 ("This administrative change . . . meant that a CFIUS determination may no longer be a final decision, and it added a new level of uncertainty to foreign investors seeking to acquire U.S. firms.").

81. See id. (describing FINSA).

82. Id.

83. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §§ 1701–1728, 132 Stat. 1653, 2174–2207 (2018) (codified at 50 U.S.C. §§ 4501, 4565 (Supp. III 2021)); see also Jackson, supra note 15, at 11 (noting concerns about "China's growing investment in the United States, particularly in the technology sector").

84. § 1702(b)(4), 132 Stat. at 2175.

In FIRRMA, Congress suggested six factors for CFIUS to consider in evaluating national security risk, including whether transactions involve "a country of special concern" that has a "strategic goal of acquiring" critical technology or infrastructure; the national security effects of patterns of transactions by foreign governments or persons; whether a transaction "is likely to expose, either directly or indirectly, personally identifiable information, genetic information, or other sensitive data of [U.S.] citizens to access by a foreign government or foreign person that may exploit that information" to threaten national security; and whether a transaction will "exacerbat[e] or creat[e] new cybersecurity vulnerabilities in the United States or is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activity against the United States."[85]

To address these concerns, FIRRMA made some significant changes to CFIUS's authorities, including expanding the scope of transactions subject to CFIUS review, making the previously all-voluntary filing system mandatory for certain transactions, and discriminating among countries involved in transactions.

Expanded Scope. To broaden the scope of transactions subject to CFIUS review, FIRRMA redefined "covered transaction," which delimits the scope of CFIUS's jurisdiction, to reach beyond the traditional definition of transactions through which foreign persons could acquire "control" of a U.S. business.[86] FIRRMA expanded CFIUS's jurisdiction "by explicitly adding four types of transactions as covered transactions":

> (1) The purchase or lease by, or concession to, a foreign person of certain real estate in the United States; (2) noncontrolling 'other investments' that afford a foreign person an equity interest in and specified access to information in the possession of, rights in, or involvement in the decisionmaking of certain U.S. businesses involved in certain critical technologies, critical infrastructure, or sensitive personal data; (3) any change in a foreign person's rights if such change could result in foreign control of a U.S. business or any other investment in certain U.S. businesses; and (4) any other transaction, transfer, agreement, or arrangement, the structure of which is designed or intended to evade or circumvent [CFIUS review].[87]

---

85. Id. § 1702(c), 132 Stat. at 2176–77.

86. 50 U.S.C. § 4565(a)(4). One of this Essay's authors has argued that the CFIUS process preempts attempts by U.S. states to add additional national security–related restrictions to deals within CFIUS's jurisdiction. See Kristen E. Eichensehr, CFIUS Preemption, 13 Harv. Nat'l Sec. J. 1 (2022).

87. Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. 50,174, 50,174 (Sept. 24, 2019) (codified at 31 C.F.R. pt. 800 (2020)); see also 50 U.S.C. § 4565(a)(4)(B); U.S. Dep't of the Treasury, Summary of the Foreign Investment Risk Review Modernization Act of 2018, at 1, https://home.treasury.gov/

CFIUS review of noncontrolling "other investments" is limited to investments in businesses that are involved with critical technologies or critical infrastructure or that "maintain[] or collect[] sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[88] CFIUS refers to these as "TID U.S. businesses," standing for "Technology, Infrastructure, and Data."[89]

Mandatory Filing. FIRRMA empowered CFIUS to shift from the voluntary filing system to mandatory filing for certain transactions.[90] CFIUS regulations have implemented this authority by requiring mandatory filing for certain transactions dealing with TID U.S. businesses that are involved in critical technologies subject to export control regulations and transactions through which a foreign person would acquire a "substantial interest" in a TID U.S. business and a foreign government holds a "substantial interest" in such foreign person.[91] The regulations define "substantial interest" to mean that the foreign person is acquiring at least a 25% voting interest (whether direct or indirect) in the TID U.S. business, and a foreign government has a 49% or greater voting interest (direct or indirect) in the foreign person.[92] For parties that are required to and fail to file, the regulations specify a civil penalty of up to "$250,000 or the value of the transaction, whichever is greater."[93]

Significantly, the mandatory filing requirements are subject to exceptions, including for certain "excepted foreign states,"[94] discussed in more detail below.

Discriminating Among States. FIRRMA also changed CFIUS's authority by allowing it to differentiate more explicitly between states. The "sense of Congress" factors mentioned above opened the door to CFIUS considering whether a "transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security."[95] Ultimately, CFIUS's regulations "do not target any particular country for greater scrutiny"—an

---

system/files/206/Summary-of-FIRRMA.pdf [https://perma.cc/45QV-WFQG] [hereinafter U.S. Dep't of the Treasury, Summary of FIRRMA] (last visited Oct. 5, 2022).

88. 50 U.S.C. § 4565(a)(4)(B)(iii); see also Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. at 50,176 (discussing the scope of "covered investments").

89. Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. at 50,176; see also 31 C.F.R. § 800.248 (defining "TID U.S. business").

90. See 50 U.S.C. § 4565(b)(1)(C)(v)(IV) ("Mandatory declarations"); see also Jackson, supra note 15, at 19–20 (discussing FIRRMA's provision of authority for mandatory filing).

91. 31 C.F.R. § 800.401.

92. Id. § 800.244 (defining "substantial interest").

93. Id. § 800.901.

94. See id. § 800.401(b)(1).

95. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1702(c)(1), 132 Stat. 1653, 2176 (2018).

issue that was "a major topic of congressional debate during consideration of FIRRMA"—but they do establish benefits for certain foreign governments, termed "excepted foreign states," and for investors from those countries.[96] Effective in February 2020, CFIUS deemed Australia, Canada, and the United Kingdom "excepted foreign states" based on "their robust intelligence-sharing and defense industrial base integration mechanisms with the United States," and it added New Zealand to this list in January 2022.[97] The list of excepted foreign states now includes all members of the Five Eyes intelligence sharing alliance (and no other countries).[98]

Going forward, a state will have to satisfy additional criteria to maintain or obtain excepted status,[99] namely whether the state "has established and is effectively utilizing a robust process to analyze foreign investments for national security risks and to facilitate coordination with the United States on matters relating to investment security."[100] In guidance on its website, CFIUS lists more specific factors including, among others: "the extent to which the foreign state possesses legal authority to review foreign investment transactions"; "whether the foreign state" has authority to and does "impose conditions on, prevent, or, if already consummated, unwind, foreign investment transactions to protect its national security"; "the extent to which the foreign state monitors and enforces compliance by parties to a foreign investment transaction with conditions the foreign state has imposed on such transaction"; and whether the foreign state has the legal authority to share information with the U.S. government about security analyses of investments.[101] CFIUS has

96. Jackson, supra note 15, at 20; see also 31 C.F.R. § 800.218 ("Excepted foreign state"); id. § 800.219 ("Excepted investor").

97. Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112, 3116 (Jan. 17, 2020); see also 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 [https://perma.cc/469Y-RZQM] (last visited Oct. 6, 2022) (showing effective dates of excepted foreign state status); Fact Sheet: Final Regulations Modifying the Definitions of Excepted Foreign State and Excepted Real Estate Foreign State and Related Actions, U.S. Dep't of the Treasury: Off. of Pub. Affs. (Jan. 5, 2022), https://home.treasury.gov/system/files/206/Fact-Sheet-Final-Rule-Revising-EFS-Definitions-2.pdf [https://perma.cc/E29C-PDD2] (noting the addition of New Zealand).

98. For background on the Five Eyes alliance among the United States, United Kingdom, Australia, Canada, and New Zealand, and intelligence sharing among them, see Scarlet Kim, Diana Lee, Asaf Lubin & Paulina Perlin, Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us About Intelligence-Sharing Agreements, Lawfare (Apr. 23, 2018), https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing [https://perma.cc/BJ2V-WQS5].

99. See 31 C.F.R. §§ 800.218, 800.1001.

100. Id. § 800.1001.

101. Factors for Determinations Under § 800.1001(a) / § 802.1001(a), U.S. Dep't of the Treasury, https://home.treasury.gov/system/files/206/Excepted-Foreign-State-Factors-for-Determinations.pdf [https://perma.cc/3S7A-FB6G] (last visited Oct. 6, 2022).

already determined that the Five Eyes member states meet these criteria and will remain excepted foreign states.[102]

Beyond statutory changes to CFIUS's jurisdiction and processes, the executive branch has echoed Congress's concerns about the "evolving national security landscape and the nature of the investments that pose related risks to national security."[103] In September 2022, President Joseph Biden issued an executive order to "sharpen" CFIUS's focus on "emerging risks."[104] Echoing Congress's suggestions in FIRRMA,[105] the order directs CFIUS, in reviewing particular transactions, to consider "five specific sets of factors," including the "transaction's effect on the resilience of critical U.S. supply chains," a transaction's impact on "U.S. technological leadership," trends in investments that reveal a threat when considered in the aggregate but not necessarily when viewed in isolation, cybersecurity risks, and risks to the sensitive data of U.S. persons.[106]

The concerns about evolving risks and the need to consider patterns of investment rather than isolated transactions also underlie U.S. advocacy for the second way in which national security–based reviews of transactions are expanding, namely the global proliferation of CFIUS-like processes, discussed in the next section.

---

102. Determination Regarding Excepted Foreign States, 88 Fed. Reg. 9190, 9190 (Feb. 13, 2023); Determination Regarding Excepted Foreign States, 87 Fed. Reg. 731, 731 (Jan. 6, 2022).

103. Exec. Order No. 14,083, 87 Fed. Reg. 57,369, 57,369 (Sept. 20, 2022).

104. Background Press Call on President Biden's Executive Order on Screening Inbound Foreign Investment, The White House (Sept. 15, 2022), https://www.whitehouse.gov/briefing-room/press-briefings/2022/09/15/background-press-call-on-president-bidens-executive-order-on-screening-inbound-foreign-investments-2/ [https://perma.cc/WA97-TAD5]; see also Exec. Order No. 14,083, 87 Fed. Reg. at 57,369–74.

105. See supra note 85 and accompanying text.

106. Fact Sheet: President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States, The White House (Sept. 15, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/ [https://perma.cc/H3LS-2VE9]; see also Exec. Order 14,083, 87 Fed. Reg. at 57,370–73. The order's expressed concern about foreign governments' access to U.S. persons' data echoes earlier government statements. For example, in announcing the indictment of Chinese military officials for hacking credit-reporting bureau Equifax, then–Attorney General William Barr noted that the Equifax intrusion "is of a piece with other Chinese illegal acquisitions of sensitive personal data," including breaches of the U.S. Office of Personnel Management, Marriott, and Anthem, and asserted that "these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages." William P. Barr, U.S. Att'y Gen., Remarks: Indictment of Four Members of China's Military for Hacking Into Equifax (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military [https://perma.cc/N8FU-9P8M] ("[T]he deliberate, indiscriminate theft of vast amounts of sensitive personal data of civilians, as occurred here, cannot be countenanced.").

2. *Global Diffusion of CFIUS-Like Processes.* — The United States is actively encouraging other countries to establish CFIUS-like processes to review foreign investments implicating national security.[107] Congress in FIRRMA expressed its sense that "the President should conduct a more robust international outreach effort to urge and help allies and partners of the United States to establish processes that are similar to [CFIUS] to screen foreign investments for national security risks and to facilitate coordination."[108] As explained above, FIRRMA codified benefits in the form of treatment as "excepted foreign states" for countries that institute CFIUS-like review systems.

Whether because of U.S. encouragement or based on their own security assessments, numerous governments have established, expanded, or intensified systems for reviewing foreign investment in the last few years.[109] Several examples illustrate this trend.

European Union. In March 2019, the European Union adopted a regulation on screening foreign direct investment (FDI) into its member states and began to apply it in October 2020.[110] Although the regulation

---

107. See, e.g., The White House, National Strategy for Critical and Emerging Technologies 9 (2020), https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf [https://perma.cc/K385-9TE5] (listing, as a Trump Administration "priority action," the plan to "[e]ngage allies and partners to develop their own processes similar to those executed by the Committee on Foreign Investment in the United States (CFIUS)"); Antony J. Blinken, Sec'y of State, Remarks at Stanford University: A Conversation on the Evolution and Importance of Technology, Diplomacy, and National Security With the 66th Secretary of State Condoleezza Rice (Oct. 17, 2022), https://www.state.gov/secretary-antony-j-blinken-at-a-conversation-on-the-evolution-and-importance-of-technology-diplomacy-and-national-security-with-66th-secretary-of-state-condoleezza-rice/ [https://perma.cc/BY6Q-8S82] (noting that the United States "want[s] to make sure that countries have the tools to look at those [concerning foreign] investments and decide whether this is something they want to go forward or not" and highlighting that the United States is working with the European Union); see also Thomas Freddo, Will Biden Use Every Tool Against China?, Wall St. J. (Apr. 22, 2021), https://www.wsj.com/articles/will-biden-use-every-tool-against-china-11619131634 (on file with the *Columbia Law Review*) (reporting that the Treasury Department during the Trump Administration "engaged with nearly 60 foreign allies on the importance of screening investments for national security risks").

108. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1702(b)(6), 132 Stat. 1653, 2176 (2018).

109. See, e.g., James K. Jackson & Cathleen D. Cimino-Isaacs, Cong. Rsch. Serv., IF10952, CFIUS Reform Under FIRRMA 2 (2020) (detailing investment review–related actions, including blocking of deals, by Canada, China, the European Commission, Germany, and the United Kingdom); see generally Sarah Bauerle Danzman & Sophie Meunier, The Big Screen: Mapping the Diffusion of Foreign Investment Screening Mechanisms (Sept. 27, 2021) (unpublished manuscript), https://ssrn.com/abstract=3913248 [https://perma.cc/5JRV-2XNA] (chronicling the recent proliferation of investment screening mechanisms in Organisation for Economic Co-operation and Development countries).

110. Commission Regulation 2019/452 of Mar. 19, 2016, Establishing a Framework for the Screening of Foreign Direct Investments Into the Union, 2019 O.J. (L 79 I) 6, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:079I:FULL&from=EN [https://perma.cc/VC63-HPTP] [hereinafter Commission Regulation 2019/452]; id. art. 17 (specifying that the "Regulation shall apply from 11 October 2020"). "Foreign" for

recognizes member states' responsibility for their national security and does not require them to establish FDI screening mechanisms, it "establishes a framework" for states to screen FDI "on the grounds of security or public order and for a mechanism for cooperation between Member States, and between Member States and the [European] Commission, with regard to foreign direct investments likely to affect security or public order."[111] The regulation establishes a cooperation mechanism whereby member states must notify the European Commission and other member states of investments that are undergoing national screening, and other affected member states or the Commission can then provide input to the state doing the screening.[112] The regulation also provides a number of factors that member states and the Commission may consider in determining whether an investment affects security or public order, including whether the foreign investor is controlled by a foreign government, whether there is a "serious risk that the foreign investor engages in illegal or criminal activity," potential effects on critical infrastructure and technologies, or "access to sensitive information, including personal data, or the ability to control such information."[113] The regulation explicitly permits international cooperation, specifying that "Member States and the Commission may cooperate with the responsible authorities of third countries on issues relating to the screening of foreign direct investments on grounds of security and public order."[114]

The Commission has encouraged member states to establish or expand FDI screening mechanisms,[115] and a growing number of states have done so.[116] As of October 2020, fifteen E.U. member states had FDI

---

purposes of the regulation means "[c]ases where the acquisition of an EU target involves direct investment by one or more entities established outside the Union." Eur. Comm'n, Frequently Asked Questions on Regulation (EU) 2019/452 Establishing a Framework for the Screening of Foreign Direct Investments Into the Union § II.12, https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157945.pdf [https://perma.cc/AE7M-ZLD7] [hereinafter Eur. Comm'n, FAQs] (last updated June 22, 2021) (emphasis omitted).

111. Commission Regulation 2019/452 art. 1.

112. Id. art. 6; see also id. art. 9 (listing information that the member state undertaking screening must provide to other states and the Commission). Specifically, the Commission may issue an opinion to the member state doing the screening when "the Commission considers that a foreign direct investment undergoing screening is likely to affect security or public order in more than one Member State, or has relevant information in relation to that foreign direct investment." Id. art. 6(3).

113. Id. art. 4.

114. Id. art. 13.

115. Communication From the Commission: Guidance to the Member States Concerning Foreign Direct Investment and Free Movement of Capital From Third Countries, and the Protection of Europe's Strategic Assets, Ahead of the Application of Regulation (EU) 2019/452 (FDI Screening Regulation), at 1–2, COM (2020) 1981 final (Mar. 25, 2020), https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158676.pdf [https://perma.cc/X4UR-DFZT].

116. See, e.g., François-Charles Laprévote, Richard Pepper, Séverine Schrameck, Aurèle Delors, Giuseppe Scassellati-Sforzolini, Francesco Iodice, Michael Ulmer & Mirko von

screening mechanisms in place,[117] and by June 2021, the number had increased to eighteen states.[118]

United Kingdom. In November 2020, the U.K. government proposed a new National Security and Investment Act (NSIA), which was adopted in April 2021 and fully entered into force in January 2022.[119] Touted as "the biggest shake-up in the UK's industrial intervention policy for nearly two decades,"[120] the NSIA introduces a mandatory notification system for certain transactions in seventeen "core" sectors, including artificial intelligence, communications, computing hardware, data infrastructure, defense, and satellite and space technologies, and it gives the government authority to "call-in" investments, both within and outside of those sectors, for review of national security risks.[121]

The NSIA also creates a voluntary notification system for parties that think their transaction might raise national security risks, and both mandatory and voluntary notices are filed with a new division of the Department for Business, Energy, and Industrial Security called the

---

Bieberstein, Cleary Gottlieb, Alert Memorandum: EU Foreign Direct Investment Regulation Comes Into Force 4 (2020), https://www.clearygottlieb.com/-/media/files/alert-memos-2020/eu-foreign-direct-investment-regulation-comes-into-force.pdf [https://perma.cc/FP6X-GU4R] ("[F]our Member States introduced new regimes in 2020 (Austria, Hungary, Poland, and Slovenia); others (including Germany, Italy, and Spain) introduced new measures in response to the COVID-19 pandemic following encouragement from the Commission; and several other countries are actively considering new legislation (including Belgium, Ireland, and Sweden)." (citation omitted)).

117. Peter Camesasca, Horst Henschen & Katherine Kingsbury, New Era of FDI in the European Union—EU FDI Regulation Now in Full Force and Effect, Covington Competition (Oct. 13, 2020), https://www.covcompetition.com/2020/10/new-era-of-fdi-in-the-european-union-eu-fdi-regulation-now-in-full-force-and-effect/ [https://perma.cc/C7LD-PTTN].

118. Eur. Comm'n, FAQs, supra note 110, § III.18 & n.4; see also Eur. Comm'n, List of Screening Mechanisms Notified by Member States 1 (2022), https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf [https://perma.cc/GM5F-KXA7] (listing eighteen member states as of May 2022).

119. See UK FDI: National Security & Investment Law Is Approved by Parliament, Covington & Burling LLP (May 3, 2021), https://www.cov.com/en/news-and-insights/insights/2021/05/uk-fdi-national-security-and-investment-law-is-approved-by-parliament [https://perma.cc/7QGF-5GXK] [hereinafter Covington & Burling LLP, UK FDI]. For the full text of the NSIA, see National Security and Investment Act 2021, c. 25 (UK), https://www.legislation.gov.uk/ukpga/2021/25/enacted [https://perma.cc/9E76-WKKN].

120. Dan Sabbagh, Ministers Seek to Stop 'Back Door' Foreign Takeovers With New Security Bill, Guardian (Nov. 10, 2020), https://www.theguardian.com/business/2020/nov/11/ministers-seek-to-stop-back-door-foreign-takeovers-with-new-security-bill [https://perma.cc/WK6Y-ZQ5C].

121. See Covington & Burling LLP, UK FDI, supra note 119 (describing the NSIA); John Schmidt, Jeremy Willcocks, Ludovica Pizzetti & Zeno J. Frediani, A New Mandatory UK Foreign Direct Investment Regime Gets Royal Assent: The Five Key Things You Need to Know, Arnold & Porter Kaye Scholer LLP (May 10, 2021), https://www.arnoldporter.com/en/perspectives/publications/2021/05/a-new-mandatory-uk-fdi-regime-gets-royal-assent [https://perma.cc/DB93-U574].

Investment Security Unit.[122] Like CFIUS, the NSIA gives the U.K. government authority to "impose conditions and, as a last resort, block transactions that it believes pose risk to UK national security."[123] As examples of possible conditions that could be imposed, the government has cited "altering the amount of shares an investor is allowed to acquire, restricting access to commercial information, or controlling access to certain operational sites or works."[124] In addition, "transactions subject to mandatory filing obligations and completed without clearance will be deemed void," and the government may "call-in" non-notified transactions for up to five years after closing (or six months after the government becomes aware of the transaction).[125] The NSIA carries substantial penalties for noncompliance, including fines, corporate criminal penalties, and up to five years' jail time for directors and officers.[126]

Prior to the NSIA, the United Kingdom had limited authority to review transactions for national security concerns as part of broader authority to screen transactions on public interest grounds pursuant to the Enterprise Act 2002,[127] but it had intervened for national security reasons only twelve times since 2002.[128] The government estimates that the new NSIA will result in 1,000 to 1,830 notifications per year, with an additional seventy to ninety-five investments called in by the government, and remedies imposed in "[a]round 10" cases.[129]

---

122. Covington & Burling LLP, UK FDI, supra note 119; Schmidt et al., supra note 121. For an overview of the process, see Department for Business, Energy & Industrial Strategy, Guidance: Check if You Need to Tell the Government About an Acquisition that Could Harm the UK's National Security (July 20, 2021) (UK), https://www.gov.uk/guidance/national-security-and-investment-act-guidance-on-acquisitions (on file with the *Columbia Law Review*) (last updated Apr. 14, 2022).

123. Schmidt et al., supra note 121.

124. Press Release, Department for Business, Energy & Industrial Strategy & Rt. Hon. Sir Alok Sharma MP, New Powers to Protect UK From Malicious Investment and Strengthen Economic Resilience (Nov. 11, 2020) (UK), https://www.gov.uk/government/news/new-powers-to-protect-uk-from-malicious-investment-and-strengthen-economic-resilience (on file with the *Columbia Law Review*).

125. Covington & Burling LLP, UK FDI, supra note 119.

126. Id.

127. See, e.g., Nicole Kar, Mark Daniel & Sofia Platzer, CFIUK? UK Introduces National Security and Investment Bill, Linklaters (Nov. 11, 2020), https://www.linklaters.com/en/insights/publications/2020/november/cfiuk-uk-introduces-national-security-and-investment-bill [https://perma.cc/G7LD-6DCJ] (discussing the Enterprise Act 2002 and the history of national security review).

128. Department for Business, Energy & Industrial Strategy, Impact Assessment, National Security and Investment Bill 11 (2020) (UK), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf [https://perma.cc/5DE2-QDNW].

129. Id. at 22.

The U.K. government has already put its new powers to use. In July 2022, it used the NSIA authority for the first time to block a transaction.[130] Then in November 2022, in what was seen as "one of the first major test cases" of the NSIA,[131] the United Kingdom ordered a Chinese-controlled company, Nexperia BV, to unwind its 2021 acquisition of a British computer chip company.[132] Nexperia has pledged to appeal the order, but "[t]here is little precedent for how the company could successfully overturn the decision."[133]

Australia. After tightening foreign investment review on national security grounds for several years,[134] Australia announced a major reform to

130. Department for Business, Energy & Industrial Strategy, National Security and Investment Act 2021: Publication of Notice of Final Order (July 20, 2022) (UK), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092802/aquisition-scamp5-scamp7-know-how-final-order-notice-20220720.pdf [https://perma.cc/69AU-SNLZ] (blocking Beijing Infinite Vision Technology Co. Ltd. from acquiring vision-sensing technology from the University of Manchester); see also Tim Castorina, Tara Rudra & Mark Daniel, First Deal Blocked Under UK's NSIA, Linklaters (July 21, 2022), https://www.linklaters.com/en/insights/blogs/foreigninvestmentlinks/2022/july/first-deal-blocked-under-uks-nsia [https://perma.cc/KL47-FQLZ] (reporting on the order).

131. See Stu Woo, U.K. to Probe Chinese-Led Takeover of Chip Maker, Wall St. J. (May 25, 2022), https://www.wsj.com/articles/u-k-to-probe-chinese-led-takeover-of-chip-maker-11653502675 (on file with the *Columbia Law Review*) (discussing review of Nexperia's acquisition of Newport Wafer Fab).

132. Department for Business, Energy & Industrial Strategy, National Security and Investment Act 2021: Publication of Notice of Final Order (Nov. 16, 2022) (UK), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118369/NWF_Final_Order_Public_Notice_16112022.pdf [https://perma.cc/4KJ3-9BFZ] (directing the acquiring company, Nexperia BV, to sell the 86% interest it acquired in the former Newport Wafer Fab in 2021); see also Alistair MacDonald, U.K. Orders Chinese-Owned Company to Unwind Chip-Factory Deal, Wall St. J. (Nov. 17, 2022), https://www.wsj.com/articles/u-k-orders-chinese-owned-company-to-unwind-chip-factory-deal-11668685510 (on file with the *Columbia Law Review*) (discussing the divestment order). Reportedly, U.S. officials lobbied the U.K. government to unwind the deal, MacDonald, supra, which had also drawn the attention of U.S. congressmen, see Sion Barry, U.S. Congressmen Call for Chinese Takeover of Welsh Tech Firm Newport Wafer Fab to Be Overturned on Security Grounds, BusinessLive (UK) (Apr. 21, 2022), https://www.businesslive.co.uk/enterprise/congressmen-call-chinese-takeover-welsh-23742183 [https://perma.cc/S6K3-YY9C].

133. Jasper Jolly, Blocking Chinese Takeover of UK Chip Firm 'Bad News' for Wales, Says Boss, Guardian (UK) (Nov. 17, 2022), https://www.theguardian.com/business/2022/nov/17/blocking-chinese-takeover-nexperia-uk-chip-firm-bad-news-for-wales-says-head [https://perma.cc/PAK5-5CBT].

134. Liz Alderman, Wary of China, Europe and Others Push Back on Foreign Takeovers, N.Y. Times (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/business/china-europe-canada-australia-deals.html (on file with the *Columbia Law Review*) ("In 2015, the [Australian] government strengthened foreign acquisitions and takeover rules to require the approval of a national oversight board [for certain transactions]."); 2020 Investment Climate Statements: Australia, U.S. Dep't of State, https://www.state.gov/reports/2020-investment-climate-statements/australia/ [https://perma.cc/6FGJ-ZEKH] (last visited Oct. 6, 2022) (discussing Australia's "steps to increase the analysis of national security implications of foreign investment in certain sectors" since 2017).

its foreign investment review system in June 2020,[135] with the changes effective at the start of 2021.[136] Australia amended its Foreign Acquisitions and Takeovers Act 1975 in 2020 to require approval by the Treasurer of foreign persons engaging in "notifiable national security actions," including acquiring interests in national security businesses or land with a connection to national security.[137] "[N]ational security business[es]" include, among others, critical infrastructure, telecommunications, defense and intelligence technology, and businesses that have classified information or personal information of defense or intelligence personnel that, if compromised, could impair national security.[138] The new legislation also gives the Australian Treasurer a "call-in" power to initiate review of any transactions, including those outside national security businesses, that the Treasurer feels may pose national security concerns.[139] Moreover, the legislation grants the Treasurer a "last resort power" that allows the Treasurer, subject to certain safeguards, "to impose conditions, vary existing conditions, or, as a last resort, require the divestment of any approved investment where national security risks emerge."[140] The 2020 legislation significantly increased the penalties for noncompliance with the screening mechanisms, including failing to comply with a requirement to obtain prior approval or breaching conditions of approval.[141]

---

135. Josh Frydenberg, Major Reforms to Australia's Foreign Investment Framework (Media Release, The Treasury, June 5, 2020) (Austl.), https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/major-reforms-australias-foreign-investment-framework [https://perma.cc/78L9-UKC4].

136. See Significant Changes to Australia's Foreign Investment Framework Commenced on 1 January 2021, Jones Day (Jan. 2021), https://www.jonesday.com/en/insights/2021/01/significant-changes-to-australias-foreign-investment-framework-commenced-on-1-january-2021 [https://perma.cc/7YLR-JDJJ] [hereinafter Jones Day, Changes to Australia's Foreign Investment Framework].

137. For an overview of the changes, see id. For the relevant statutory provisions, see Foreign Acquisitions and Takeovers Act 1975 (Cth) pt III (Austl.), https://www.legislation.gov.au/Details/C2022C00088 [https://perma.cc/U5YF-NZP3].

138. Foreign Acquisitions and Takeovers Regulation 2015 (Cth) pt I s 8AA (Austl.), https://www.legislation.gov.au/Details/F2022C00395 [https://perma.cc/CR36-MVFR] (defining "national security business"); see also Foreign Investment Review Board, National Security (Guidance: 8, Apr. 12, 2022) 4–5 (Austl.), https://firb.gov.au/sites/firb.gov.au/files/guidance-notes/GN08_NationalSecurity_1.pdf (on file with the *Columbia Law Review*) [hereinafter Austl. FIRB Guidance] (same).

139. Austl. FIRB Guidance, supra note 138, at 11 ("The Treasurer can 'call-in' for review reviewable national security actions which are not otherwise notified, if the Treasurer considers that the action may pose national security concerns. The review can occur when the action is still proposed or up to ten years after the action has been taken."); see also Jones Day, Changes to Australia's Foreign Investment Framework, supra note 136 (describing the Australian Treasurer's "[n]ew [c]all-in [p]ower" (emphasis omitted)).

140. Austl. FIRB Guidance, supra note 138, at 3; see also id. at 12–13 (describing the last resort power, including the conditions that will prompt its use); Jones Day, Changes to Australia's Foreign Investment Framework, supra note 136 (same).

141. See The Treasury, Foreign Investment Reforms (June 2020) 17–18 (Austl.), https://treasury.gov.au/sites/default/files/2020-06/p2020-87595_0.pdf [https://perma.cc/

As in the United States, the reforms appear motivated in large part by Chinese investments.[142] According to research by Australian National University (ANU), "Chinese investment in Australia peaked at A$16.5 billion in 2016, spanning agriculture, transport, energy utilities, healthcare, mining and property."[143] But in 2020, "Chinese investment in Australia fell by 61% . . . to the lowest level . . . in six years, coinciding with a worsening diplomatic dispute" and significantly outpacing the global decrease in FDI due to the COVID-19 pandemic.[144] According to ANU, in 2020, "just 20 new projects attracted Chinese investment, well down from a peak of 111 in 2016," and much of it came "via Australian subsidiaries rather than by foreign firms directly."[145] In November 2020, China's government issued an extensive list of "grievances" against Australia, including Australia's blocking of "more than 10 Chinese investment projects" on what Beijing called "ambiguous and unfounded national security concerns."[146]

Numerous other countries, including Canada, China, Germany, Japan, and New Zealand, have enacted or strengthened existing national

---

LGD4-TU9N] [hereinafter Austl. Treasury, Foreign Investment Reforms]; The Treasury, Foreign Investment: Compliance Framework Policy Statement (Dec. 2020) 6–9 (Austl.), https://firb.gov.au/sites/firb.gov.au/files/2021-01/FIRB_compliance_framework.pdf [https://perma.cc/F9KS-9TH2]; Jones Day, Changes to Australia's Foreign Investment Framework, supra note 136 ("For corporations, the maximum criminal penalty for residential and non-residential investments will increase from A$832,500 to A$33.3 million, and the maximum civil penalty for non-residential investments will increase from A$277,500 to A$555 million.").

142. See, e.g., Alderman, supra note 134 (discussing concerns about Chinese investments in Australia); Anthony Galloway, National Security Concerns Thwart Chinese Bid for Major Builder, Sydney Morning Herald (Jan. 12, 2021), https://www.smh.com.au/politics/federal/national-security-concerns-thwart-chinese-bid-for-major-builder-20210112-p56tez.html [https://perma.cc/CD54-6MFJ] (noting that the Australian government "rejected a takeover bid for one of Australia's largest builders from a Chinese government controlled company over concerns it could give foreign intelligence services access to information about the nation's critical infrastructure").

143. Chinese Investment in Australia Plummets Amid Tensions, Reuters (Feb. 28, 2021), https://www.reuters.com/world/china/chinese-investment-australia-plummets-amid-tensions-2021-02-28/ [https://perma.cc/4XEU-HL69].

144. Id.

145. Paul Karp, Chinese Investment in Australia Plunged by 61% Last Year, New Data Shows, Guardian (Feb. 28, 2021), https://www.theguardian.com/australia-news/2021/mar/01/chinese-investment-in-australia-plunged-by-61-last-year-new-data-shows [https://perma.cc/3D4G-BJSW].

146. Jonathan Kearsley, Eryk Bagshaw & Anthony Galloway, 'If You Make China the Enemy, China Will Be the Enemy': Beijing's Fresh Threat to Australia, Sydney Morning Herald (Nov. 18, 2020), https://www.smh.com.au/world/asia/if-you-make-china-the-enemy-china-will-be-the-enemy-beijing-s-fresh-threat-to-australia-20201118-p56fqs.html [https://perma.cc/MZ3E-EDSC] (internal quotation marks omitted) (quoting a list of grievances from the Chinese government); see also Karp, supra note 145 (listing examples of deals involving China that the Australian government has blocked, including "the proposed sale of Australia's largest landholder, S Kidman & Co, which comprises 1.3% of Australia's total land mass; the proposed $600m takeover of Lion Dairy; and a $300m bid for a major Victorian construction contractor").

security reviews of foreign investments in recent years.[147] It remains to be seen how such reviews might be coordinated across countries or whether clearance (or blocking) of an investor or investment in one interested country might affect the investor's prospects in other countries' processes.

3. *Increased U.S. Restrictions on Outbound Investment.* — National security creep is evident not just with respect to inbound investment screening but also in new restrictions and potential forthcoming restrictions on outbound investment from the United States.[148]

In November 2020, then-President Donald Trump issued Executive Order 13,959 on "Addressing the Threat From Securities Investments that Finance Communist Chinese Military Companies."[149] The order explained that "[t]hrough the national strategy of Military-Civil Fusion," China "increases the size of the country's military-industrial complex by compelling civilian Chinese companies to support its military and intelligence activities[,]"[150] while such companies "raise capital by selling securities to United States investors that trade on public exchanges both here and abroad, lobbying United States index providers and funds to include these securities in market offerings, and engaging in other acts to ensure access to United States capital."[151] This strategy allows China, the order alleged, to "exploit[] United States investors to finance the

147. Austl. Treasury, Foreign Investment Reforms, supra note 141, at 3 (summarizing changes to foreign investment screening mechanisms by the United States, European Commission, Japan, China, and New Zealand); see also Alderman, supra note 134 (discussing changes to Canadian law); Tobias Buck, Germany Toughens Investment Rules as China Concerns Build, Fin. Times (Dec. 19, 2018), https://www.ft.com/content/568183dc-038e-11e9-99df-6183d3002ee1 (on file with the *Columbia Law Review*) (describing reforms to tighten national security screening of foreign investments in Germany); Melissa Eddy, Germany Blocks 2 Foreign Investment Deals, Taking a Firmer Line on China, N.Y. Times (Nov. 9, 2022), https://www.nytimes.com/2022/11/09/world/europe/germany-china-investment.html (on file with the *Columbia Law Review*) (reporting that the German government blocked two investments by Chinese companies on security grounds); Gearoid Reidy & Shoko Oda, Japan Moves to Limit Foreign Investment in Half of Listed Firms, Bloomberg (May 10, 2020), https://www.bloomberg.com/news/articles/2020-05-11/japan-moves-to-limit-foreign-investment-in-half-of-listed-firms#xj4y7vzkg (on file with the *Columbia Law Review*) (last updated May 11, 2020) (discussing changes to national security screening of investments into Japan and noting that they "are most likely to target foreign state-owned enterprises, with Chinese investment in the country a particular source of concern").

148. Outbound investment restrictions and screening mechanisms may not be limited to the United States. See European Commission, Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Work Programme 2023, at 8, COM (2022) 548 final (Oct. 18, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0548&qid=1666271020857 [https://perma.cc/W2PC-T7KB] (noting that the Commission "will examine whether additional tools are necessary in respect of outbound strategic investment controls" (emphasis omitted)).

149. Exec. Order No. 13,959, 85 Fed. Reg. 73,185 (Nov. 17, 2020) (codified at 3 C.F.R. 475 (2021)).

150. Id. at 73,185.

151. Id.

development and modernization of its military."[152] Citing the IEEPA and NEA, among other authorities, the order prohibited U.S. persons from engaging in "any transaction in publicly traded securities, or any securities that are derivative of, or are designed to provide investment exposure to such securities, of any Communist Chinese military company," effective January 11, 2021.[153] The order gave U.S. investors until November 2021 to divest from prohibited securities.[154] The companies included in the order came from a list compiled by the Secretary of Defense[155] and included "prominent Chinese technology, manufacturing and infrastructure companies, such as China Mobile Communications Group, China Telecommunications Corporation, Huawei, Sinochem Group, Hangzhou Hikvision Digital Technology, China Railway Construction Corporation, Inspur Group and Aviation Industry Corporation of China."[156]

After two Chinese companies won preliminary injunctions in federal court in challenges to their inclusion on the Defense Department's list,[157] the Biden Administration issued a new executive order that shifted responsibility for identifying companies to the Treasury Department but otherwise retained and broadened the Trump Administration order.[158] The new order covers not just Chinese companies supporting the Chinese military but also threats from "the development or use of Chinese surveillance technology."[159] It prohibits U.S. persons from engaging in transactions of securities of entities that the Treasury Secretary determines "operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of the PRC," or entities that own or control such companies or are owned or controlled by them.[160]

The White House explained that the order "allows the United States to prohibit—in a targeted and scoped manner—U.S. investments in Chinese companies that undermine the security or democratic values of

152. Id.

153. Id.

154. Id. at 73,186.

155. Id.

156. Ana Swanson, Trump Bars Investment in Chinese Firms With Military Ties, N.Y. Times (Nov. 12, 2020), https://www.nytimes.com/2020/11/12/business/economy/trump-china-investment-ban.html (on file with the *Columbia Law Review*) (last updated June 3, 2021).

157. See Karen Freifeld, Update 1—Nasdaq Withdraws Listing Ban on Luokung After U.S. Judge's Decision, Reuters (May 6, 2021), https://www.reuters.com/article/usa-china-luokung-tech-idCNL1N2MT26H [https://perma.cc/9M4Z-U3T3] (reporting preliminary injunctions won by Luokung Technology Corp. and Xiaomi Corporation against their inclusion on the investment ban list).

158. Exec. Order No. 14,032, 86 Fed. Reg. 30,145 (June 3, 2021) (codified at 3 C.F.R. 586 (2022)).

159. Id. at 30,145.

160. Id. The order permitted U.S. persons to divest from prohibited investments by June 3, 2022, or within a year after a company is added to the prohibition list. Id. at 30,146.

the United States and our allies."[161] An annex to the order listed fifty-nine entities subject to the investment prohibition.[162] The list includes many, like China Mobile Communications Group, China Telecommunications Corporation, and Huawei, that were on the Trump Administration list, but it also adds new companies and omits others.[163] The Biden Administration subsequently added additional companies to the list and is reportedly considering issuing an executive order to impose additional restrictions on U.S. investment into Chinese companies that work on quantum computing, artificial intelligence, and other technologies that could have military applications.[164]

Congress, too, is considering broader restrictions on outbound investment, specifically establishing an interagency committee colloquially called "outbound CFIUS" or "reverse CFIUS."[165] Congress considered and

---

161. Fact Sheet: Executive Order Addressing the Threat From Securities Investments that Finance Certain Companies of the People's Republic of China, The White House (June 3, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/03/fact-sheet-executive-order-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/ [https://perma.cc/6FP6-PSC2].

162. Annex to Exec. Order No. 14,032, 86 Fed. Reg. 30,148, 30,148–49 (June 3, 2021) (codified at 3 C.F.R. 586, 589 (2022)). For the latest version of the list, see Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List), U.S. Dep't of the Treasury, https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list [https://perma.cc/GG6M-HDZY] (last updated Dec. 16, 2021).

163. For a helpful breakdown of companies that were included in both orders or in only one or the other, see Paul, Weiss, Rifkind, Wharton & Garrison LLP, President Biden Revamps Communist Chinese Military Companies (CCMC) Sanctions Program 7–10 (2021), https://www.paulweiss.com/media/3981164/president_biden_revamps_communist_chinese_military_companies_ccmc_sanctions_program.pdf [https://perma.cc/4JAT-T6QV]. Among the companies omitted from the Biden Administration list are Luokung Technology Corp. and Xiaomi Corporation, see id., the two that had won preliminary injunctions against their inclusion on the Trump Administration list, see Freifeld, supra note 157. For more on the order, see David E. Sanger & David McCabe, Biden Expands Trump-Era Ban on Investment in Chinese Firms Linked to Military, N.Y. Times (June 3, 2021), https://www.nytimes.com/2021/06/03/us/politics/biden-ban-chinese-firms-trump.html (on file with the *Columbia Law Review*).

164. Press Release, U.S. Dep't of the Treasury, Treasury Identifies Eight Chinese Tech Firms as Part of the Chinese Military-Industrial Complex (Dec. 16, 2021), https://home.treasury.gov/news/press-releases/jy0538 [https://perma.cc/FU56-NWS6]; see also Ellen Nakashima & Jeanne Whalen, Biden Administration Concerned About U.S. Investments in Chinese Tech Companies With Military or Surveillance Ties, Wash. Post (Dec. 16, 2021), https://www.washingtonpost.com/national-security/us-investments-china-biden/2021/12/15/835876a0-5772-11ec-a808-3197a22b19fa_story.html (on file with the *Columbia Law Review*) (discussing concerns in the Biden Administration and possible "narrowly tailored" regulation of outbound investments); Hans Nichols, Scoop: White House Narrowing Executive Order on China Investments, Axios (Jan. 12, 2023), https://www.axios.com/2023/01/12/white-house-biden-china-executive-order-cfius [https://perma.cc/9GGD-AV4L] (reporting on deliberations within the Biden Administration about the scope of the upcoming executive order and suggesting that the order "will focus more on quantum computing, artificial intelligence and semiconductors and not include biotechnology or battery technology").

165. See, e.g., Sarah Bauerle Danzman, Is the US Going to Screen Outbound Investment?, Atl. Council: Econographics (Jan. 10, 2022), https://www.atlanticcouncil.org/

rejected screening outbound investment in 2018,[166] but in 2021, new outbound screening proposals garnered bipartisan support. Senators Bob Casey (D-PA) and John Cornyn (R-TX) introduced the "National Critical Capabilities Defense Act" to establish an interagency committee—the Committee on National Critical Capabilities (CNCC)—to screen outbound investments on national security grounds.[167] The CNCC would review transactions by U.S. businesses that shift to a country of concern or transfer to an entity of concern crucial elements of "national critical capabilities" or that pose "unacceptable risk to a national critical capability."[168] Like CFIUS, the bill would also empower the President to take actions to mitigate risks, up to and including prohibiting transactions or seeking divestment.[169] The sponsors intend the bill to "establish a whole-of-government process to screen outbound investments and the offshoring of critical capacities and supply chains to foreign adversaries, like China and Russia, to ensure the resiliency of critical supply chains."[170]

Of note, as compared to the existing CFIUS regime, the proposed CNCC regime further conflates national security and economic interests. In particular, the CNCC would have the authority to review transactions relating to "national critical capabilities," broadly defined to include a wide range of activities, such as those involving manufacturing and advanced packaging, quantum information science, artificial intelligence, and "other industries, technologies, and supply chains which may be

---

blogs/econographics/is-the-us-going-to-screen-outbound-investment/ [https://perma.cc/E4DQ-6M47] (discussing "outbound CFIUS"); Dan Primack, Congress May Regulate U.S. Investor Activity in China, Axios (June 15, 2022), https://www.axios.com/2022/06/15/congress-may-regulate-us-investor-activity-in-china [https://perma.cc/A4LS-22V4] (discussing "reverse CFIUS").

166. See Shawn Donnan, Senators Ditch Plan to Review US Outbound Investments, Fin. Times (May 15, 2018), https://www.ft.com/content/a1fcfeec-57cf-11e8-bdb7-f6677d2e1ce8 (on file with the *Columbia Law Review*).

167. Casey and Cornyn Release a Joint Statement on National Critical Capabilities Defense Act, Bob Casey: U.S. Sen. for Pa. (May 24, 2021), https://www.casey.senate.gov/news/releases/casey-and-cornyn-release-a-joint-statement-on-national-critical-capabilities-defense-act [https://perma.cc/3LWY-MLC2] [hereinafter Casey & Cornyn, Joint Statement].

168. See 167 Cong. Rec. S3269–72 (daily ed. May 20, 2021) (text of Senate Amendment 1853) (defining covered transaction and describing CNCC review). The bill defines "country of concern" as having the same meaning as "foreign adversary" in a separate statutory provision: "any foreign government or foreign nongovernment person engaged in a long term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons." Id. at S3268, S3270 (identified in § 1001(4)); see also 47 U.S.C. § 1607(c)(2) (Supp. III 2021) (defining "foreign adversary"); Mario Mancuso & Luci Hague, What Outbound Investment Reviews Would Mean for US Cos., Law360 (June 17, 2022), https://www.law360.com/articles/1503969 (on file with the *Columbia Law Review*).

169. 167 Cong. Rec. at S3271 (described in § 1004).

170. Casey & Cornyn, Joint Statement, supra note 167.

identified by the CNCC."[171] Although the White House endorsed outbound screening,[172] the compromise China competition bill, which the House and Senate negotiated in July 2022, ultimately omitted the outbound screening process.[173] Nonetheless, the significant bicameral and bipartisan support the CNCC garnered suggests that Congress may revisit an outbound screening mechanism in the near future, perhaps adding to executive branch actions.[174]

* * *

Building on the descriptive account set out in this Part, the next Part identifies theoretical implications of the expanding creep of national security reviews of corporate deals, including some implications specific to CFIUS-like contexts and others that reach more broadly, touching on questions common to other national security–related commercial regulations.

II. THEORETICAL IMPLICATIONS

Much has been said about the impact of regulation on national security and corporate transactions. In the corporate and contract theory literature, for instance, regulations are understood not only to add to dealmaking costs but also to provide opportunities for arbitrage and value creation.[175] But as the previous Part discussed, national security–related regulation differs in many ways from other types of regulation, even when

171. James Mendenhall, Michael E. Borden, Justin R. Becker, Carys Golesworthy & Grigore Alexandru, Senators Introduce Compromise Proposal Regarding Review of Outbound Investment, Sidley Austin LLP (June 23, 2022), https://www.sidley.com/en/insights/publications/2022/06/senators-introduce-compromise-proposal-regarding-review-of-outbound-investment [https://perma.cc/8RVS-NBVH].

172. Ellen Nakashima, White House Wants Transparency on American Investment in China, Wash. Post (July 13, 2022), https://www.washingtonpost.com/national-security/2022/07/13/china-investment-transparency/ (on file with the *Columbia Law Review*) (reporting Biden Administration support).

173. John D. McKinnon, Senate Bill to Boost Chip Production, Advanced Technology Set to Move Ahead, Wall St. J. (July 26, 2022), https://www.wsj.com/articles/senate-bill-to-boost-chip-production-advanced-technology-set-to-move-ahead-11658741402 (on file with the *Columbia Law Review*) (last updated July 27, 2022) (noting omission of outbound investment screening); see also CHIPS and Science Act, Pub. L. No. 117-167, 136 Stat. 1366 (2022).

174. See, e.g., Nichols, supra note 164 (discussing a draft executive order on outbound investment restrictions); Revised National Critical Capabilities Defense Act of 2022 Proposes Expansive Outbound Investment Review Regime, Covington & Burling LLP (June 16, 2022), https://www.cov.com/en/news-and-insights/insights/2022/06/revised-national-critical-capabilities-defense-act-of-2022-proposes-expansive-outbound-investment-review-regime [https://perma.cc/SP4A-TFHB] (noting "significant, bipartisan support for enacting some form of outbound investment review regime" and the prospect of its inclusion in other bills or adoption of a process via executive order going forward).

175. See, e.g., Victor Fleischer, Regulatory Arbitrage, 89 Tex. L. Rev. 227, 238 (2010) (describing how deal lawyers can assist clients in designing deals that create better regulatory treatment).

it is not "creeping": National security is by necessity sensitive and secretive, contributing to a number of regulatory quirks that other regulatory systems lack.

This Part highlights two theoretical implications of national security creep: its potential to alter when and how judges defer to factual and legal claims by the executive branch and its complication of dealmaking and contract theory.

A. *Exceptionalism and Deference in Judicial Review*

As the account of national security creep in Part I makes clear, the authorities the U.S. government exercises in this sphere come from the combined action of Congress and the executive. This is not a circumstance where the executive has grabbed power at the expense of Congress. Rather, Congress has repeatedly provided broad authorities to the executive branch and pushed the executive to use them, and the executive is doing so robustly. Part of the reason Congress has recently expanded the executive's authorities with respect to CFIUS and may do the same for the proposed outbound CFIUS process is the broad bipartisan support for countering China's efforts to compete with the United States on technology and innovation—a rare point of cross-party consensus in today's fraught political environment.

For those interested in the separation of powers, however, the unity of effort across the executive and legislative branches raises some caution flags. A Congress seemingly pushing the executive to exercise power may not scrupulously monitor that such power is used properly, and an executive pushed to use delegated authorities (and to use them in secret) by the branch doing the delegating may be less careful than it would be if facing robust critical oversight. In a Madisonian sense, ambitions are not counteracting one another, but fostering one another.[176] Moreover, the process of national security creep is also not being cabined by a "separation of parties"—which some argue is as or more important than the separation of powers—because of widespread bipartisan agreement over national security creep.[177] The apparent absence of some of the typical constitutional and political checks on executive action raises questions about what other oversight of national security creep may be available. Two main possibilities spring to mind: the judiciary and the public.[178]

---

176. The Federalist No. 51, at 398 (James Madison) (John C. Hamilton ed., 1864).

177. Daryl J. Levinson & Richard H. Pildes, Separation of Parties, Not Powers, 119 Harv. L. Rev. 2311, 2329–30 (2006) (identifying the "Separation of Parties" and arguing that "[t]o the extent constitutional law is concerned with the real as opposed to the parchment government, it would do well to shift focus from the static existence of separate branches to the dynamic interactions of the political parties that animate those branches").

178. Other actors may also be in a position to serve as checks. Regulated companies can push back against government claims within the CFIUS process or by taking the government to court, and foreign governments, including, for example, those whose companies are

Judges have a role to play in overseeing national security creep. This section identifies three ways in which judges might react to the executive broadening its claims about what counts as national security: quietly expand the deference they typically give to the executive on national security to meet the expanded scope of claims, constrict deference to the executive on national security across the board, or bifurcate deference based on whether the executive's claim involves "traditional" areas of national security or the economically focused ones on which this Essay focuses. Such adjustments to judicial practice have important implications not just for the executive and regulated parties but also for ongoing scholarly debates about the extent to which national security and foreign relations are subject to exceptional rules or instead "normalized" toward a baseline of domestic law.[179] This section focuses on the role of the judiciary in reviewing discrete instances of national security creep, while the Conclusion addresses the role of the public, and particularly scholars.

1. *Judicial Responses to Expanding National Security Claims.* — As the third branch of the federal government, the judiciary is an obvious possibility to consider when thinking about oversight of executive action on national security. At the same time, the role of judges in national security oversight is often limited in important ways: The judiciary can only consider cases properly before it, and problems with standing and the political question doctrine, among other issues, often cabin the judiciary's ability to address the substantive merits of national security disputes.[180] With respect to national security creep, however, these doctrines may not be much of a barrier. Because the regulatory actions this Essay addresses operate on private parties, such parties will often have standing and a ripe dispute to put before the judiciary. Moreover, their claims do not obviously raise political questions and are likely to be based on statutory claims, which at least some judges have been reluctant to hold raise political questions.[181]

Even if case and controversy requirements can be satisfied, however, another limitation on the judiciary's role in national security disputes comes from judges' practice of reviewing executive claims deferentially. Deference is a broad and slippery term that can describe everything from

---

caught up in regulatory review, might also question or push back against U.S. government actions. Cf. Ashley Deeks, Secrecy Surrogates, 106 Va. L. Rev. 1395 (2020) (highlighting the role of technology companies, states and localities, and foreign allies as "secrecy surrogates" that can check U.S. executive branch abuses of secrecy).

179. See infra notes 228–237 and accompanying text.

180. See, e.g., Clapper v. Amnesty Int'l U.S.A., 568 U.S. 398, 401–02 (2013) (holding that U.S. citizen plaintiffs lacked standing to challenge government surveillance programs); Jaber v. United States, 861 F.3d 241, 250 (D.C. Cir. 2017) (holding that a lawsuit about a U.S. drone strike was barred by the political question doctrine).

181. See, e.g., Zivotofsky v. Clinton, 566 U.S. 189, 196–97 (2012) (holding that determining the constitutionality of a statute about place of birth on passports did not pose a political question).

giving the government's view preferential consideration to substantial weight to dispositive acceptance.[182] In foreign affairs cases, courts have deployed multiple kinds of deference to the executive.[183] Such deference may pose a greater hurdle than limitations on jurisdiction and justiciability for parties hoping that the judiciary will provide robust oversight of national security creep issues and ensure that executive actions in the name of national security are well founded.

Deference, however, is not necessarily static. Will judges change their behavior in response to national security creep–related claims, and if so, how? Three main possibilities emerge. The first is that judges simply accept the executive's expanding claims about what constitutes national security and remain deferential in national security–related cases for the same reasons that they have traditionally cited. The result would be a *quiet expansion* of deference. The second and third possibilities posit changes in judges' approaches to deference, albeit of different types. The second possibility—call it *constriction*—is that ever-broader claims about what falls within the ambit of national security, particularly the economically focused claims at issue in national security creep, cause judges to become more skeptical of and less deferential to executive branch national security assertions across the board, even on more traditional national security–related issues like terrorism or war powers. The third possibility is that judges engage in *bifurcation* of national security–related issues, continuing to treat traditional national security–related issues with their customary levels of deference, while becoming more skeptical of and less deferential to executive claims based on broader conceptions of national security like those at issue in this Essay.

Normatively, which approach one supports likely depends on one's more general views about deference to the executive branch—a debate beyond the scope of this Essay. We focus here on the predictive and descriptive, setting out the arguments in favor of each of the three outcomes before offering some preliminary thoughts as to which is most likely.

The *quiet expansion* possibility, in which judges continue on their current trajectory of deference to the executive branch in national security cases, is perhaps the easiest of the options to explain. There are reasons to think that, even in the national security creep context, judges may defer to the executive branch and thus provide only limited external oversight

182. See, e.g., Peter L. Strauss, "Deference" Is Too Confusing—Let's Call Them "*Chevron* Space" and "*Skidmore* Weight", 112 Colum L. Rev. 1143, 1145 (2012) ("'[D]eference' is a highly variable, if not empty, concept . . . sometimes used in the sense of 'obey' or 'accept,' and sometimes as 'respectfully consider.'").

183. See Bradley, *Chevron* Deference and Foreign Affairs, supra note 22, at 659–63 (identifying "five overlapping categories" of foreign affairs deference); Eichensehr, Foreign Sovereigns as Friends of the Court, supra note 22, at 326–51 (discussing justifications for and kinds of deference afforded to the executive branch and foreign sovereign amici in foreign relations cases).

of national security creep. The courts have long afforded deference to agencies' statutory interpretations,[184] and the statutes the executive often cites as authority for its restrictions on inbound and outbound investments—statutes such as the CFIUS statute, IEEPA, and the NEA—are rife with scope for executive discretion. The CFIUS statute, for example, leaves the crucial term "national security" undefined, giving the Treasury Department, the White House, and CFIUS agencies tremendous flexibility for interpretation.[185] Similarly, IEEPA authority depends on a presidential determination that there is an "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."[186]

Beyond statutory interpretation, courts also routinely defer to the executive branch on factual determinations about foreign relations and

---

184. See United States v. Mead Corp., 533 U.S. 218, 226–28 (2001) (explaining when agency interpretations receive *Chevron* deference); Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 842–43 (1984) (setting out the two-step inquiry for deference to an agency's statutory interpretation); Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944) (explaining that the "weight" courts give to an agency's view "depend[s] upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control").

These and other administrative law deference doctrines are in significant flux. For example, last term the Supreme Court did not overrule—but also did not cite—*Chevron* in a case about Medicare reimbursements. See Am. Hosp. Ass'n v. Becerra, 142 S. Ct. 1896 (2022); see also James Romoser, In an Opinion that Shuns *Chevron*, the Court Rejects a Medicare Cut for Hospital Drugs, SCOTUSblog (June 15, 2022), https://www.scotusblog.com/2022/06/in-an-opinion-that-shuns-chevron-the-court-rejects-a-medicare-cut-for-hospital-drugs/ [https://perma.cc/UR7Z-MDVC] (noting that although "hundreds of pages of briefing and a large chunk of the oral argument focused on the continued vitality of" *Chevron*, "the court might simply snuff out *Chevron* with the silent treatment"). Even more fundamentally, several Justices have proposed reinvigorating the nondelegation doctrine to cabin the scope of congressional delegations to executive agencies. See Gundy v. United States, 139 S. Ct. 2116, 2137–42 (2019) (Gorsuch, J., dissenting) (criticizing the Court's current "intelligible principle" test for nondelegation); see also Paul v. United States, 140 S. Ct. 342, 342 (2019) (Kavanaugh, J., statement respecting the denial of certiorari) (suggesting agreement with Gorsuch's opinion in *Gundy* regarding the nondelegation doctrine). Notably, however, Justices who advocate reinvigorating the nondelegation doctrine have suggested that certain circumstances, including delegations to the executive branch to engage in factfinding and delegations relating to foreign relations, may continue even as courts narrow the scope of other delegations. *Gundy*, 139 S. Ct. at 2136–37 (Gorsuch, J., dissenting). If this revolution in administrative law comes to pass, foreign relations and national security may look even more exceptional. Cf. Harlan Grant Cohen, The National Security Delegation Conundrum, Just Sec. (July 17, 2019), https://www.justsecurity.org/64946/the-national-security-delegation-conundrum/ [https://perma.cc/434V-U6M8] (considering the foreign relations law implications of reinvigorating the nondelegation doctrine).

185. 50 U.S.C. § 4565(a) (Supp. III 2021); cf. E. Maddy Berg, Note, A Tale of Two Statutes: Using IEEPA's Accountability Safeguards to Inspire CFIUS Reform, 118 Colum. L. Rev. 1763, 1792–94 (2018) (suggesting that CFIUS should clarify how it defines national security).

186. 50 U.S.C. § 1701(a).

national security.[187] Judges rely on functional justifications for such "national security fact deference,"[188] including the executive branch's expertise (and the court's comparative lack of expertise) on issues of foreign relations and national security and the executive branch's access to additional sources of information.[189]

The Supreme Court has been particularly deferential in circumstances where *predictive* judgments about national security are involved.[190] In *Department of the Navy v. Egan*, for example, the Supreme Court deferred to the executive in reviewing the denial of a security clearance application,

187. See, e.g., Holder v. Humanitarian L. Project, 561 U.S. 1, 33–34 (2010) (explaining, in a case challenging application of the material support to terrorism statute, that "evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference" when "sensitive and weighty interests of national security and foreign affairs" are involved); Jama v. Immigr. & Customs Enf't, 543 U.S. 335, 348 (2005) (citing the Supreme Court's "customary policy of deference to the President in matters of foreign affairs"); Webster v. Doe, 486 U.S. 592, 600 (1988) (determining that a statute permitting the CIA Director to terminate a CIA employee "whenever the Director 'shall *deem* such termination necessary or advisable in the interests of the United States' . . . fairly exudes deference to the Director, and . . . foreclose[s] the application of any meaningful standard of judicial review" (quoting National Security Act of 1947, Pub. L. No. 80-253, § 102(c), 61 Stat. 495, 498)); Bradley, *Chevron* Deference and Foreign Affairs, supra note 22, at 661–62 (discussing judicial deference to the executive on "international facts"); Chesney, supra note 22, at 1366–85 (describing examples of national security fact deference in practice); Eichensehr, Foreign Sovereigns as Friends of the Court, supra note 22, at 329–31 (discussing expertise-based deference to the executive on factual determinations). This Essay discusses deference on foreign relations and national security–related facts interchangeably because the categories overlap significantly, including on foreign investment issues. Cf. Deeks, supra note 22, at 875–76 (noting the overlap between kinds of deference in foreign affairs and national security cases).

188. Chesney, supra note 22, at 1362 (defining "national security fact deference" as the practice of "judges defer[ring] to factual judgments made by the executive branch in litigation involving national security").

189. See, e.g., *Holder*, 561 U.S. at 34 (explaining the Court's deference to factual assessments by the executive about terrorism on the grounds that "neither the Members of this Court nor most federal judges begin the day with briefings that may describe new and serious threats to our Nation and its people" (internal quotation marks omitted) (quoting Boumediene v. Bush, 553 U.S. 723, 797 (2008))); id. ("[W]hen it comes to collecting evidence and drawing factual inferences in this area [of terrorism designations], 'the lack of competence on the part of the courts is marked'" (quoting Rostker v. Goldberg, 453 U.S. 57, 65 (1981))); Chesney, supra note 22, at 1405–11 (discussing information access and expertise justifications for national security fact deference); Jean Galbraith & David Zaring, Soft Law as Foreign Relations Law, 99 Cornell L. Rev. 735, 773 (2014) (noting that courts' deference to the executive branch on foreign relations is "[t]ypically grounded in functionalist justifications").

190. Bradley, *Chevron* Deference and Foreign Affairs, supra note 22, at 661 (noting that the issues of "international facts" on which courts "typically" defer to the executive sometimes "have a strong empirical or predictive component"); Chesney, supra note 22, at 1409–10 (arguing that "[e]xpertise often will matter a great deal when it comes to predictive factfinding in the national security setting," including instances "such as whether disclosure of a particular secret would be harmful to national security"); Eichensehr, Foreign Sovereigns as Friends of the Court, supra note 22, at 336 (discussing the Supreme Court's expertise-based rationales for deference to the executive on predictive fact questions).

concluding that the decision involved an "attempt to predict [a person's] possible future behavior" and that "[p]redictive judgment of this kind must be made by those with the necessary expertise in protecting classified information."[191] The Court noted that "it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment and to decide whether the agency should have been able to make the necessary affirmative prediction with confidence" or to "determine what constitutes an acceptable margin of error in assessing the potential risk."[192] One might characterize a foreign investor's future intentions to exploit vulnerabilities in U.S. businesses as a similar predictive judgment on which judges would defer to the executive's expertise and superior information.

Judges are also not divorced from the political environment, where there is bipartisan support for executive branch action to counter perceived threats stemming from China on technology issues in particular.[193] Some judges might well defer to national security claims based on their approach to executive power, their perception of the reasonableness of the claims, and the state of national security threats to the United States. A constant drumbeat of headlines warns about the decline of U.S. global power, the rise of China as a competitor and adversary, and the risk for national security, businesses, and individuals from cybersecurity compromises.[194] In such circumstances, executive branch claims that Chinese companies' access to sensitive personal data or technologies must be restricted

---

191. 484 U.S. 518, 528–29 (1988).

192. Id. at 529; see also *Holder*, 561 U.S. at 35 ("The Government, when seeking to prevent imminent harms in the context of international affairs and national security, is not required to conclusively link all the pieces in the puzzle before we grant weight to its empirical conclusions.").

193. See, e.g., Richard Fontaine, Washington's Missing China Strategy, Foreign Affs. (Jan. 14, 2022), https://www.foreignaffairs.com/articles/china/2022-01-14/washingtons-missing-china-strategy (on file with the *Columbia Law Review*) ("Jettisoning Washington's previous strategy of cooperation and integration [with China], premised as it was on the eventual transformation of Chinese behavior, is a rare point of agreement between the Trump and Biden administrations."); cf. National Security Strategy, supra note 29, at 32 ("Technology is central to today's geopolitical competition and to the future of our national security, economy and democracy.").

194. See, e.g., Julian E. Barnes, China Poses Biggest Threat to U.S., Intelligence Report Says, N.Y. Times (Apr. 13, 2021), https://www.nytimes.com/2021/04/13/us/politics/china-national-security-intelligence-report.html (on file with the *Columbia Law Review*); Michèle A. Flournoy, America's Military Risks Losing Its Edge, Foreign Affs. (Apr. 20, 2021), https://www.foreignaffairs.com/articles/united-states/2021-04-20/flournoy-americas-military-risks-losing-its-edge (on file with the *Columbia Law Review*); Zolan Kanno-Youngs & David E. Sanger, U.S. Accuses China of Hacking Microsoft, N.Y. Times (July 19, 2021), https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html (on file with the *Columbia Law Review*) (last updated Aug. 26, 2021); Tom McTague, The Decline of the American World, Atlantic (June 24, 2020), https://www.theatlantic.com/international/archive/2020/06/america-image-power-trump/613228/ [https://perma.cc/6VFZ-4DUF].

to protect national security could find a deferentially disposed audience in the judiciary.[195]

Despite these reasons suggesting continued deference to the executive branch on and a limited role for the judiciary in overseeing national security creep–related actions, countervailing reasons suggest that judicial behavior might shift in line with the *constriction* and *bifurcation* possibilities described above. The countervailing reasons come from changes in the kinds of cases that are presented to the judiciary and from how judges react to such claims.

The U.S. government's expanded conception of national security may prompt more and different challenges to national security–motivated actions. Companies that view themselves as peripheral to or simply not involved in national security are increasingly likely to be caught up in national security reviews, and unlike defense contractors and other companies in traditional national security–sensitive lines of business, these companies may be more willing to challenge executive actions against them.[196] Other challenges may come from companies that concede that they are involved in sensitive businesses but regard their limited ties to the United States as insufficient to warrant CFIUS jurisdiction.[197] Companies caught up in the outbound investment restrictions may be particularly likely to challenge their inclusion on investment ban lists because they have not had a prior opportunity to engage with the government and negotiate like parties to transactions reviewed by CFIUS have.

Moreover, companies caught up in expanded claims of national security may have different kinds of claims to bring and different plaintiffs situated to bring them. For example, in summer 2020, the Trump Administration issued executive orders that directly implicated TikTok and WeChat, two Chinese smartphone apps, alleging data security concerns and attempting effectively to force the apps to shut down operations in the United States and to force TikTok's Chinese parent company to divest itself of the app.[198] WeChat users and TikTok users and content creators sued to challenge the orders, citing both statutory and constitutional

---

195. Cf. Curtis A. Bradley, Foreign Relations Law and the Purported Shift Away From "Exceptionalism", 128 Harv. L. Rev. Forum 294, 303 (2015) [hereinafter Bradley, Foreign Relations Law] ("[I]f the shift to normalization was initiated because of a sense immediately after the end of the Cold War that foreign relations had become less dangerous and consequential, it is not clear why the shift should be expected to continue after the emergence of new threats, such as global terrorism and heightened geopolitical struggles with countries like Russia and China.").

196. See infra notes 216–226 and accompanying text (discussing successful challenges by Xiaomi and Luokung to their designation as companies affiliated with China's military).

197. Cf. infra notes 308–312 (discussing CFIUS review of the Magnachip deal).

198. See Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 11, 2020) (codified at 3 C.F.R. 414 (2021)) (WeChat); Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 11, 2020) (codified at 3 C.F.R. 412 (2021)) (TikTok). For a description of the orders and resulting litigation, see generally Eichensehr, Regulatory Actions Against TikTok, supra note 43.

claims, including First and Fifth Amendment protections.[199] And TikTok's parent company, ByteDance, argued that the statutory exemptions in IEEPA for "information or informational materials" and "personal communication" rendered the Administration's actions impermissible.[200] The lawsuits resulted in multiple preliminary injunctions against the government from several district courts across the country.[201]

Beyond changes in what kinds of claims and cases are presented to courts is the question of how judges then react to them. When previously exceptional claims of national security–related deference become more pervasive, do judges alter their treatment of executive claims for deference?

One could imagine judges becoming more skeptical of and less deferential to government arguments about national security in general. This is the second possibility noted above, namely, *constriction*, which results in decreased deference on national security claims across the board.

Some have argued that, for judges, "[f]requency leads to normalcy,"[202] and so the more frequent and less exceptional national security issues become, the more comfortable judges become adjudicating claims. For example, judges faced with frequent national security–related claims may come to see less comparative expertise in the executive branch, rating more highly their own competence to assess risks. Or seeing the executive branch make more frequent claims of national security risk could lead to more skepticism among judges about whether the risks are as real or as significant as the executive claims. Think of this as the boy-who-cried-wolf problem. The economically focused national security creep–related claims may be particularly susceptible to skepticism of this type because they focus on longer-term and more remote risks, like losing technological leadership in artificial intelligence or quantum computing,[203] than claims related to, for example, terrorism, which are easier to articulate to judges.

---

199. See Anupam Chander, Trump v. TikTok, 55 Vand. J. Transnat'l L. 1145, 1156–61 (2022) (discussing litigation challenging the orders against TikTok and WeChat); Eichensehr, Regulatory Actions Against TikTok, supra note 43, at 126–29 (same).

200. Eichensehr, Regulatory Actions Against TikTok, supra note 43, at 127–28 (discussing lawsuit by TikTok parent company ByteDance).

201. See id. at 126–29 (describing these preliminary injunctions); see also TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 96 (D.D.C. 2020); Marland v. Trump, 498 F. Supp. 3d 624, 645 (E.D. Pa. 2020); TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 76 (D.D.C. 2020); U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 917 (N.D. Cal. 2020).

202. Ganesh Sitaraman & Ingrid Wuerth, The Normalization of Foreign Relations Law, 128 Harv. L. Rev. 1897, 1903 (2015).

203. Cf. Exec. Order No. 14,083, 87 Fed. Reg. 57,369, 57,371 (Sept. 20, 2022) (directing CFIUS to consider whether a transaction implicates "United States technological leadership and therefore national security" in areas including "microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies").

The third possibility noted above—*bifurcation*—also posits a change in judges' willingness to defer, but instead of decreased deference across the board, it focuses on dividing national security claims into "traditional" areas of national security versus the economically focused restrictions that make up national security creep, with deference decreasing only for the latter category. Judges might effectively develop a hierarchy of national security–related claims wherein they treat executive assertions regarding more traditional national security issues with more deference than newer sorts of assertions about the necessity of national security–related restrictions on economic activity. This alternative avoids expanding the scope of issues on which courts defer to the executive, while also not disrupting existing exceptional treatment of national security–related claims in areas judges have traditionally viewed as implicating the executive's expertise and access to information.

Importantly, while either *constriction* or *bifurcation* would involve less deference or more searching review by courts, these approaches would not necessarily mean that judges would give *no* deference to the executive's national security claims, just reduced deference or increased scrutiny. Needless to say, the executive branch is unlikely to welcome such scrutiny and would need to consider how to respond, not just in particular litigation, but more broadly. The process would be iterative: If the executive knows that national security–related orders are likely to face challenge, and if they are challenged, courts will push the executive to disclose significant information to justify its actions, the executive would face a choice between pulling back on the scope and kind of national security orders it issues or disclosing more information than it might like to defend such orders in court. In this way, courts could act as *some* check—albeit an imperfect one—on national security creep, even beyond particular cases in which they issue orders.

Although there is limited case law to date, some evidence suggests that judges are pushing back against the government's economically focused national security claims.

The D.C. Circuit laid the groundwork for such questioning when it held in *Ralls Corp. v. CFIUS* in 2014 that limited judicial review is available for adverse CFIUS actions, despite language in the CFIUS statute specifying that presidential actions to suspend or prohibit transactions and findings that a foreign investor might impair national security "shall not be subject to judicial review."[204] Ralls Corporation, a U.S. company owned by two Chinese nationals, acquired several companies engaged in developing windfarms near a U.S. Navy base and notified CFIUS only after concluding the acquisitions, claiming that they did not pose a national security

204. 758 F.3d 296, 308–12 (D.C. Cir. 2014); see also 50 U.S.C. §§ 4565(d)(1), (d)(4), (e)(1) (2021).

threat.[205] CFIUS disagreed.[206] The President ordered Ralls to divest itself of the acquired companies.[207] Ralls sued CFIUS and the President, arguing, among other claims, that the mitigation measures CFIUS had ordered and the divestment order violated the Administrative Procedure Act (APA) and the company's Fifth Amendment due process rights.[208] After rejecting the government's argument that the case presented a political question,[209] the D.C. Circuit determined that the CFIUS statute's text and legislative history did not "provide[] clear and convincing evidence that the Congress intended to preclude judicial review of Ralls's procedural due process challenge," as opposed to the substantive outcome of the divestment decision.[210] Citing the Supreme Court's decision in *Mathews v. Eldridge*,[211] the court held that "due process requires, at the least, that an affected party be informed of the official action, be given access to the unclassified evidence on which the official actor relied and be afforded an opportunity to rebut that evidence."[212] The government's failure to provide Ralls with such process was "a clear constitutional violation, notwithstanding the [government's] substantial interest in national security and despite [the court's] uncertainty that more process would have led to a different presidential decision."[213]

When TikTok filed a petition for review in the D.C. Circuit challenging the divestment order issued by President Trump in 2020, the company cited *Ralls*.[214] TikTok's case remains pending but is currently being held in abeyance at the parties' request.[215]

In the past two years, courts have also proven willing to scrutinize national security–related restrictions on companies outside the CFIUS process and to rule in favor of companies challenging adverse national security–related actions, at least at the preliminary injunction stage. In

---

205. *Ralls Corp.*, 758 F.3d at 304–05.

206. Id. at 305.

207. Id. at 306.

208. Id.

209. Id. at 314.

210. Id. at 311; see also id. ("The text does not . . . refer to the reviewability of a constitutional claim challenging the process preceding such presidential action.").

211. Id. at 317–18 (citing Mathews v. Eldridge, 424 U.S. 319, 335 (1976)).

212. Id. at 319.

213. Id. at 320; cf. Will Gent, Note, Tilting at Windmills: National Security, Foreign Investment, and Executive Authority in Light of *Ralls Corp. v. CFIUS*, 94 Or. L. Rev. 455, 483 (2016) (characterizing *Ralls* as "considerably less deferential to the executive than other national security-related decisions"). After remand to the district court, the government and Ralls settled the case, and Ralls sold the companies. Stephen Dockery, Chinese Company Will Sell Wind Farm Assets in CFIUS Settlement, Wall St. J., https://www.wsj.com/articles/BL-252B-8621 (on file with the *Columbia Law Review*) (last updated Nov. 4, 2015).

214. Petition for Review at 2, TikTok Inc. v. Comm. on Foreign Inv. in the U.S., No. 20-1444 (D.C. Cir. filed Nov. 10, 2020).

215. Order, *TikTok Inc.*, No. 20-1444 (D.C. Cir. filed Feb. 19, 2021).

2021, a federal district court granted preliminary injunctions to two Chinese companies that challenged their inclusion on the Trump Administration's list of companies linked to China's military in which U.S. persons are prohibited from investing. The first case was brought by Xiaomi Corporation, a "multinational consumer electronics corporation" that produces smartphones, TVs, and laptops.[216] While recognizing that courts generally afford agencies heightened deference in national security–related matters,[217] the court nonetheless concluded that Xiaomi's designation by the Department of Defense (DOD) violated the APA due to inadequate explanation and lack of "substantial evidence," among other issues.[218] In weighing the equities of whether to issue the preliminary injunction, the district court expressed considerable skepticism about the national security interests the government cited. The judge noted that the statutory designation authority "went unused for almost twenty years until a flurry of designations were made in the final days of the Trump administration," and "[t]his lack of use . . . undermines the notion that the . . . designation process is critical to maintaining this nation's security."[219]

In the second case, the district court granted a preliminary injunction to Luokung Technology Corp., which sells "navigation and mapping technology," including "in-dash car navigation systems."[220] Although noting that courts "afford heightened deference to an agency's determination when it concerns national security,"[221] the judge concluded that Luokung had shown a likelihood of success on the merits.[222] The district court rejected DOD's broad interpretation of the language defining companies that could be designated[223] and concluded that the company's designation was arbitrary and capricious pursuant to the APA because it was not based on substantial evidence and exceeded DOD's statutory authority.[224] Citing DOD's reliance "not [on] any classified security intelligence" but on "a handful of innocuous facts gathered from company press releases" and "potential future contracts" with the Chinese government that "do not appear to have materialized," the court asserted that "[d]eference is only appropriate when national security interests are actually at stake, which the Court concludes is not evident here."[225] Although the judge did not reach Luokung's constitutional procedural

216. Xiaomi Corp. v. Dep't of Def., No. 21-280, 2021 WL 950144, at *2 (D.D.C. Mar. 12, 2021).

217. Id. at *4.

218. Id. at *4–8.

219. Id. at *12.

220. Luokung Tech. Corp. v. Dep't of Def., 538 F. Supp. 3d 174, 178–79 (D.D.C. 2021).

221. Id. at 182.

222. Id. at 183.

223. Id. at 183–88.

224. Id. at 188–91.

225. Id. at 195.

due process claim, he went out of his way to note that Luokung "raise[s] serious concerns" about due process and "that the Court is concerned that the Department of Defense subjected a public company to de-listing from the only stock market on which its shares were listed [Nasdaq] with no notice or process whatsoever."[226]

When combined with the several preliminary injunctions issued against the executive for its actions against TikTok,[227] these cases are part of a notable string of losses for the United States in national security–related cases. These opinions may well encourage other companies that find themselves subject to national security–related regulations to challenge the government's actions, putting it through its paces in court and perhaps even prevailing over executive actions.

2. *Nuancing the Scholarly Debate*. — Beyond the implications for particular cases, parties, and judges, cases related to national security creep will also provide grist for and perhaps add further nuance to a scholarly debate about exceptionalism and normalization in judicial review of national security and foreign relations cases. Coined by Professor Curtis Bradley,[228] the term "foreign affairs exceptionalism" refers to the idea that "domestic and foreign affairs–related issues are analyzed in distinct ways as a matter of function, doctrine, or methodology."[229] This exceptionalism manifests in a variety of ways, such as increased deference to the executive branch in foreign relations and national security cases and robust deployment of justiciability doctrines, like the political question doctrine, to preclude judicial review of the merits of such cases.[230]

Professors Ganesh Sitaraman and Ingrid Wuerth have argued that the Supreme Court is in the process of "normalizing" its previously exceptional treatment of foreign affairs cases.[231] They described the rise of foreign relations exceptionalism in the early twentieth century and its

---

226. Id. at 191 n.13; see also id. at 193 (noting that Luokung shares only trade on Nasdaq).

227. See supra notes 198–201 and accompanying text.

228. Curtis A. Bradley, The Treaty Power and American Federalism, 97 Mich. L. Rev. 390, 461 (1998) (coining the term "foreign affairs exceptionalism" for an "approach" that "distinguishes sharply between domestic and foreign affairs"); see also Curtis A. Bradley, *Breard*, Our Dualist Constitution, and the Internationalist Conception, 51 Stan. L. Rev. 529, 539 n.51 (1999) (explaining "foreign affairs exceptionalism" as "the view that the usual constitutional restraints on the federal government's exercise of power do not apply in the area of foreign affairs").

229. Sitaraman & Wuerth, supra note 202, at 1907–08.

230. See, e.g., id. at 1925–27, 1930–34 (identifying justiciability and deference to the executive as areas of exceptionality that are, in the authors' view, in the process of being normalized).

231. Id. at 1901 (arguing that "[o]ver the last twenty-five years . . . the Supreme Court has rejected the idea that foreign affairs are different from domestic affairs" and "has treated foreign relations issues as if they were run-of-the-mill domestic policy issues," resulting in "foreign relations law . . . being normalized").

subsequent dominance through the end of the Cold War[232] but argued that courts have engaged in several waves of "normalization" from the end of the Cold War and through the Roberts Court in areas including justiciability and deference to the executive.[233]

Although Sitaraman and Wuerth endorsed normalization as a normative matter,[234] their arguments prompted significant pushback. Bradley and Professor Carlos Vázquez questioned the descriptive claims about a trend toward normalization in the Supreme Court precedents Sitaraman and Wuerth cited.[235] Bradley and Professor Stephen Vladeck also focused on the extent to which exceptionalism is still prevalent in lower court decisions, including ones left undisturbed by the Supreme Court.[236] Sitaraman and Wuerth themselves identified a number of areas where "normalization is not complete," including, as relevant here, "judicial review of factual determinations made by the executive branch or by the legislature."[237]

Cases stemming from national security creep–related executive actions provide additional fodder for the normalization-versus-exceptionalism debate and will likely complicate it. The *constriction* possibility discussed above—that the increasing scope of claims about national security may prompt judges to cut back on deference to the executive across the board in national security cases—would show how claims of exceptionalism can backfire, prompting normalization in the form of decreased deference that is the opposite of what the executive seeks. Or consider the *bifurcation* possibility discussed above. In that circumstance, one might understand broadening of claims about exceptionalism on the part of the executive branch to prompt more nuanced normalization: limited or no deference on some national security–related claims but higher levels of deference on traditional national security–related issues. "Normalization" with respect to economic claims and the line drawing it might prompt could actually reinforce exceptionalism (in the form of heightened deference) with respect to more traditional national security claims.

---

232. Id. at 1913–19.

233. Id. at 1919–35.

234. Id. at 1905.

235. Bradley, Foreign Relations Law, supra note 195, at 297–301 (challenging Sitaraman and Wuerth's descriptive claims about normalization in both Supreme Court and lower court precedents); Carlos M. Vázquez, The Abiding Exceptionalism of Foreign Relations Doctrine, 128 Harv. L. Rev. Forum 305, 305 (2015) (critiquing Sitaraman and Wuerth's descriptive claim that normalization has occurred and noting that "the claim that exceptionalism is now exceptional seems overstated").

236. Bradley, Foreign Relations Law, supra note 195, at 298; Stephen I. Vladeck, The Exceptionalism of Foreign Relations Normalization, 128 Harv. L. Rev. Forum 322, 322–23 (2015) (arguing that "foreign relations exceptionalism in contemporary U.S. litigation is alive and well" in the lower federal courts).

237. Sitaraman & Wuerth, supra note 202, at 1965–66; see also Bradley, Foreign Relations Law, supra note 195, at 300 (contending that the case for normalization with respect to deference to the executive branch is mixed).

Whichever of these possibilities comes to pass, the national security creep–based cases seem likely to complicate the exceptionalism-versus-normalization discussion.

* * *

As the recent expansions in CFIUS jurisdiction and new (and possibly forthcoming) restrictions on outbound investment play out, increasing numbers of companies will find themselves on the receiving end of restrictions and will need to decide whether to challenge them.[238] Such decisions by private companies will help to determine the extent to which national security creep is presented to the judiciary and thus the extent to which judges can serve as an external check on national security creep. With respect to many areas of national security law, the judiciary plays a circumscribed role in checking the political branches.[239] The involvement of regulated private parties—including corporations with incentives and resources to challenge the government—in national security creep suggests that the judiciary may be somewhat better positioned to oversee economically focused national security–related actions, but its role remains subject to the discretion of private parties who decide whether to file cases. Thus, other mechanisms for oversight should also be considered. The Conclusion returns to the role of the public and government transparency.

B. *Challenges to the Scholarly Account of Regulators' Involvement in Corporate Deals*

The creeping nature of national security review adds new and substantial uncertainty to deals, upending well-understood contract theory about deal costs and disrupting deal planning.

In the contract theory literature, it is conventional wisdom that the cost of designing a contract includes ex ante design costs, ex post litigation costs, and some factor of judicial error.[240] What happens ex ante affects the ex post: More investment in ex ante contract design reduces the probability of ex post litigation because the resulting contract is presumably clearer, better drafted, and less prone to dispute.[241] Similarly, less investment ex ante leads to a higher probability of ex post litigation.[242] As others have compellingly argued, in some circumstances, it is rational to skimp on ex ante contract design—for example, if the probability of litigation is very low.[243]

---

238. See supra section I.B.1.

239. See supra section II.A.1.

240. Posner, supra note 26, at 1583.

241. See supra note 27 and accompanying text.

242. See supra note 27 and accompanying text.

243. See Choi & Triantis, supra note 27, at 852 (noting that if the probability of litigation is low, it may be efficient to use vague contract provisions).

In recent years, scholars have also begun to understand the role that regulators play in contract design and litigation. In previous coauthored work, one of this Essay's authors documented the phenomenon of regulator influence on contract design.[244] In business-to-consumer contracts such as internet privacy policies and terms of service, for example, contract drafters representing businesses reported that third-party regulators, not their consumer counterparties, were their most important contractual audience.[245] Other scholars have documented similar phenomena. One scholar, for instance, found that corporate contract drafters writing business-to-consumer contracts choose contract provisions as a result of policymakers' preferences.[246] Another investigated whether one policymaker's preference for a provision trickles into contracts governed by another policymaker's jurisdiction, finding that although policymakers influence what goes into bilateral contracts, there is relatively little spillover into other jurisdictions.[247]

Invariably, however, the existing literature conceives of regulators as having a single opportunity to intervene in private deals, after which parties are again left free to contract.[248] And, with very few exceptions, parties bear the cost of those regulatory interventions in the ex ante portion of the equation: They invest time and money to tango with regulators prior to the deal's closing, after which they receive certainty that the deal is allowed to go forward.

---

244. See Cathy Hwang & Matthew Jennejohn, Contractual Depth, 106 Minn. L. Rev. 1267, 1270–71 (2022) (showing through in-house counsel interviews that contract drafters often drafted contracts primarily to adhere to regulator preferences and that the preferences of consumers—their actual contract counterparties—are of second-order concern).

245. See id. at 1268.

246. See James Fallows Tierney, Contract Design in the Shadow of Regulation, 98 Neb. L. Rev. 874, 877 (2020) (arguing that contracts' audience is sometimes "regulators or policymakers, rather than consumers or courts" and that firms "may adopt contract terms that help them fend off reform" when they "anticipate legal reform that would threaten a profitable term or practice").

247. See Jens Frankenreiter, Cost-Based California Effects, 39 Yale J. on Regul. 1098, 1138–42 (2022) (finding that despite widespread claims that the European Union's pro–consumer privacy policies would spill over into non-E.U. jurisdictions, that spillover is significantly less widespread than expected for many websites).

248. One exception is a recent paper coauthored by one of this Essay's authors, which discusses the possibility of public intervention in private contracts in the litigation phase, through contract reformation. See David A. Hoffman & Cathy Hwang, The Social Cost of Contract, 121 Colum. L. Rev. 979 (2021). These last-ditch interventions, however, are rare and will continue to be; the paper argues that they are most relevant in situations where the public's share of the contract's externalities changes significantly between the contract's drafting and enforcement. Id. at 991–97 (noting that the public has several opportunities to intervene in private contracts, including ex ante through laws and regulation, midstream through regulatory approval, and, in very rare cases, ex post through contract reformation); see also Cathy Hwang, A Comment on Casey & Niblett, *The Limits of Public Contract Law*, 88 Law & Contemp. Probs. 73, 73 (2022) (describing the three ways that the public can intervene in contracts).

Antitrust review provides an apt example of this kind of common, one-and-done regulatory review that falls into the ex ante cost category. In the United States, major deals require preapproval from antitrust authorities—the Federal Trade Commission (FTC) or the Department of Justice (DOJ)—before consummation.[249] While deal parties and their antitrust lawyers complain heartily of the considerable expense, logistical nuisance, and uncertainty that antitrust review injects into a deal, antitrust regulators' effect, at least compared to the potential effect of CFIUS, is relatively self-contained and easy to calculate.[250]

Major transactions—defined by deal size, along with a few other factors—are required to file for preapproval with antitrust regulators. Once the deal parties make the filing and pay a fee, they wait. If antitrust authorities take no action after a statutorily defined several weeks, or if the authorities grant "early termination" of the waiting period, the parties can go forward with the deal.[251] Otherwise, antitrust authorities might request additional information, ask the parties to make certain modifications to ensure the deal does not have an anticompetitive outcome,[252] or seek to block the deal.[253]

While the preclearance process may not always be cheap, easy, or pleasant, deal parties understand its contours relatively well. Parties with deals of a certain size know to file for preclearance and often can predict whether regulators will approve of the deal or what changes they might request. With very few exceptions,[254] antitrust review is completed prior to deal closing, and parties can put antitrust review risks out of mind after such review is over.

Because the contours of antitrust regulator intervention are relatively well understood, parties can revert to the familiar calculations of ex ante cost, ex post cost, and judicial error to determine their anticipated contracting costs.

---

249. Hoffman & Hwang, supra note 248, at 992.

250. Of course, individual reactions to even the clearest regulation might differ, causing some uncertainty. See Claire A. Hill, Tax Lawyers Are People Too, 26 Va. Tax Rev. 1065, 1066 (2007) (noting that some regulated parties may "behave well" while others may comply by adopting "a narrow literal interpretation of a rule [that] violates its spirit").

251. Premerger Notification and the Merger Review Process, FTC, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/mergers/premerger-notification-merger-review [https://perma.cc/A6PS-VK48] [hereinafter FTC, Premerger Notification] (last visited Oct. 6, 2022).

252. See Hoffman & Hwang, supra note 248, at 992–93 (describing the divestments that antitrust authorities required before allowing the 2010 merger of United Airlines and Continental Airlines).

253. FTC, Premerger Notification, supra note 251.

254. See Cadwalader, Wickersham & Taft LLP, Buyer Beware: FTC Orders Unwinding of a Consummated Transaction 2–3 (2019), https://www.cadwalader.com/uploads/cfmemos/4a874ac35a6e26c9b3cdd46597bfd059.pdf [https://perma.cc/RV2W-DNSE] (describing eight examples of mergers that have been unwound after consummation between 2012 and 2019).

For example, parties are aware that closing certain large deals without antitrust preclearance can result in significant ex post costs: civil sanctions tied to the number of days in violation of antitrust laws or the deal being unwound.[255] Because parties are aware of the ex post costs, they can make ex ante investments to avoid those costs—that is, they can invest the significant up-front time and money to file for preclearance.

Similarly, parties that might be subject to significant antitrust review know that they are at risk and that antitrust regulators will look at publicly filed documents for clues about how a combination will result in anticompetitive behavior post-closing. They also know that if an antitrust regulator asks the parties to divest some of their assets as a precondition to regulatory approval, the question of who should divest which assets will cause a significant kerfuffle between the deal parties.[256] In order to temper these ex post risks—of significant review, of having anticompetitive potential found in public documents, and of disputes between the parties themselves about appropriate divestiture—deal parties often negotiate and memorialize their divestiture plans in private side letter agreements that, until recently, could potentially be kept from regulators.[257] These agreements are another example of ex ante investment that reduces the probability of ex post cost.

Importantly, parties can engage in this kind of exchange of costs—investing more up front to reduce ex post cost—because of three important conditions. First, even though most deals are precleared without fanfare, enough antitrust intervention has occurred that significant precedent exists about the types of potential ex post cost. Moreover, antitrust intervention is largely public: Both the FTC and DOJ issue press releases, publish public divestiture orders, and engage in public injunctions.[258] Because parties know where the potential regulatory landmines

255. The FTC Post Consummation Review Process, FTC, https://www.ftc.gov/enforcement/premerger-notification-program/post-consummation-filings-hsr-violations/ftc-post [https://perma.cc/K3ZH-ZNFJ] (last visited Oct. 6, 2022).

256. See Frequently Asked Questions About Merger Consent Order Provisions, FTC, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/frequently-asked-questions-about-merger-consent-order-provisions [https://perma.cc/T357-PQKE] (last visited Oct. 6, 2022) (discussing the divestiture-related issues that both the acquiring and acquired firms must consider during a merger).

257. See Pamela L. Taylor & Michael H. Knight, All Merger Side Letters Must Be Included in HSR Filings, Jones Day (Jan. 2018), https://www.jonesday.com/en/insights/2018/01/all-merger-side-letters-must-be-included-in-hsr-fi [https://perma.cc/HDX9-38EB].

258. See The Enforcers, FTC, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/enforcers [https://perma.cc/43Q4-BYH3] (last visited Oct. 5, 2022) (discussing FTC and DOJ enforcement mechanisms); FTC, Premerger Notification, supra note 251 (noting that agencies may "seek to stop an entire transaction by filing for a preliminary injunction in federal court"); Maria Raptis, David P. Wales & Ryan J. Travers, FTC and DOJ Enforcement Actions Highlight Scrutiny of Divestiture Orders Compliance, Skadden, Arps, Slate, Meagher & Flom LLP (Aug. 21, 2020), https://www.skadden.com/insights/publications/2020/08/ftc-and-doj-enforcement-actions [https://perma.cc/5R2H-

lie, they can invest up front to avoid them.[259] Second, antitrust authorities are clear about the types of deals in which they intervene.[260] In fact, they annually publish guidance that clearly sets out which deals need to file for preclearance.[261] Finally, for the most part, antitrust regulators predictably intervene one time in a deal—during the ex ante deal design phase.[262] After that intervention, antitrust authorities generally step back, and the parties proceed with their deal without antitrust intervention.[263]

National security review does not enjoy all of those conditions. For one thing, much of the national security review process is confidential.[264] There are many antitrust cases with detailed government briefing and judicial analysis about how best to slice and dice anticompetitive behavior, and those cases are easily accessible by the public. By contrast, there is only one published judicial opinion in a case challenging CFIUS—*Ralls v. CFIUS*—and its substantive analysis on the government's justification for

---

Z9XW] (describing recent enforcement actions); see also Justice News, DOJ, https://www.justice.gov/news [https://perma.cc/2EJN-PFTM] (last visited Oct. 12, 2022) (listing recent DOJ press releases); Press Releases, FTC, https://www.ftc.gov/news-events/news/press-releases [https://perma.cc/77B5-9FW2] (last visited Oct. 12, 2022) (listing recent FTC press releases).

259. See FTC, Premerger Notification, supra note 251 (providing detailed public guidance on FTC merger review processes and noting that FTC staff members will "answer questions and maintain a website with helpful information about how and when to file").

260. See Competitive Effects, FTC, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/competitive-effects [https://perma.cc/YX4B-8YY7] (last visited Oct. 12, 2022) (noting types of mergers in which the FTC will intervene due to their tendency to lessen competition and create monopoly); Entry and Efficiencies, FTC, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/entry-efficiencies [https://perma.cc/AF29-6KWQ] (last visited Oct. 12, 2022) (discussing the rationale for FTC challenges to mergers that will create market inefficiency or whose market harms will not be mitigated by the entry of competitors); Markets, FTC, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/markets [https://perma.cc/3JD8-CTK4] (last visited Oct. 12, 2022) (noting that "the [FTC] will examine the businesses of the merging parties both in terms of *what* they sell . . . and *where* they sell it").

261. See FTC, Premerger Notification, supra note 251.

262. See Mergers, FTC, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers [https://perma.cc/8M2L-56T3] (last visited Oct. 12, 2022) (noting that merger law relies primarily on premerger review and advanced notice to "avoid[] the difficult and potentially ineffective 'unscrambling of the eggs' once an anticompetitive merger has been completed").

263. It is rare for the government to attempt to unwind a transaction for antitrust reasons after the transaction has closed. See Elizabeth Dwoskin, Regulators Want to Break Up Facebook. That's a Technical Nightmare, Insiders Say, Wash. Post (Dec. 11, 2020), https://www.washingtonpost.com/technology/2020/12/11/facebook-breakup-antitrust/ (on file with the *Columbia Law Review*) (noting that, if successful, an FTC breakup of Facebook after its acquisitions of WhatsApp and Instagram would be "incredibly rare" and that "[t]he last time the government broke up a monopoly was in the early 1980s").

264. See U.S. Dep't of the Treasury, CFIUS, supra note 4 (explaining the review process's statutorily mandated confidentiality requirements).

ordering divestiture is slim.[265] In short, because national security is itself sensitive and often confidential, so too are orders to divest or unwind deals—leaving many future deal parties, especially those who lack counsel from experienced CFIUS attorneys, very few clues about potential regulatory landmines.

The second condition is also not met. Unlike antitrust, national security review can reach a variety of deals, including deals in industries that the government previously ignored.[266] Much of what was not regulated five years ago is now part of CFIUS's purview.[267] Much of what CFIUS has done in the last ten years has been unprecedented and therefore unexpectable by parties: CFIUS has expanded beyond industries of its historical interest, and even its orders to unwind closed deals, while always theoretically possible, came as a surprise to dealmakers when the power was ultimately used. In 2021, for instance, CFIUS asserted jurisdiction to review a deal between a Chinese private equity company and a South Korea–based semiconductor company, Magnachip.[268] Neither party had significant U.S. ties, so the parties did not preemptively seek CFIUS approval—but CFIUS asserted jurisdiction over the deal, presumably based on the semiconductor company's incorporation in Delaware and a few other relatively limited U.S. ties.[269] As a result of additional resources from the passage of FIRRMA, CFIUS has substantially increased its review of so-called "non-notified" transactions—that is, transactions where the parties did not voluntarily or mandatorily file with CFIUS pre-closing.[270] As one law firm puts it, recent CFIUS activity means that "it is simply getting harder for

265. See Ralls Corp. v. Comm. on Foreign Inv. in the U.S., 758 F.3d 296, 305, 325 (D.C. Cir. 2014) (speculating briefly on, but not evaluating, the reasons for the CFIUS order); see also supra notes 204–213 (discussing *Ralls*).

266. See supra notes 86–87 and accompanying text.

267. See U.S. Dep't of the Treasury, Summary of FIRRMA, supra note 87, at 1.

268. Brandon L. Van Grack & James Brower, CFIUS's Expanding Jurisdiction in the Magnachip Acquisition, Lawfare (Oct. 11, 2021), https://www.lawfareblog.com/cfiuss-expanding-jurisdiction-magnachip-acquisition [https://perma.cc/9YAV-RX3T].

269. See infra notes 308–312 and accompanying text.

270. CFIUS's annual report to Congress for 2020 reported that the Committee considered 117 non-notified transactions and requested that parties file in seventeen of them, CFIUS 2020 Report, supra note 62, at 48, while its 2021 report showed that the Committee considered 135 non-notified transactions and requested filings from parties in eight of them, Comm. on Foreign Inv. in the U.S., Annual Report to Congress 45 (2022), https://home.treasury.gov/system/files/206/CFIUS-Public-AnnualReporttoCongressCY2021.pdf [https://perma.cc/UDH4-QX6Q] (reporting on the calendar year 2021); see also Chase D. Kaniecki & Pete Young, A Look Behind the CFIUS Non-Notified Process Curtain; How It Works and How to Handle Outreach From CFIUS, Cleary Gottlieb: Cleary Foreign Inv. & Int'l Trade Watch (Oct. 14, 2021), https://www.clearytradewatch.com/2021/10/a-look-behind-the-cfius-non-notified-process-curtain-how-it-works-and-how-to-handle-outreach-from-cfius/ [https://perma.cc/92PW-84WP] (speculating that the number of non-notified transactions that resulted in requests for filings had increased significantly from 2018 to 2020 and noting that "we expect that many more parties to non-notified transactions will hear from CFIUS and potentially receive a request to go through the CFIUS review process").

potentially sensitive transactions to 'fly under the radar,' and the odds of CFIUS reaching out on transactions that might be of interest have increased substantially."[271]

Finally, current review processes are also temporally tentacular: CFIUS review can occur at any point during a deal's life, even after closing.[272] And, unlike other countries, where post-closing review can only occur for a few years, there is no outside limit on how long after closing CFIUS might initiate review of a deal.[273] One law firm, for instance, reported that they "have advised clients on a variety of non-notified transactions of differing sizes ranging from deals that closed nearly a decade ago to ones that have only recently signed and not yet closed."[274] The result of this expansive review, then, is that, unlike with other types of regulatory review, regulatory uncertainty around national security review does not end when the deal closes. Rather, uncertainty related to national security review has a long tail, bringing to the fore questions of how parties might need to consider or divide that uncertainty in their deals.

CFIUS's tentacular process upends contract law's well-understood trade-off between ex ante and ex post costs. When facing a regulatory regime that is as secret, unpredictable, and ever-expanding as CFIUS, parties have a hard time investing up front to reduce ex post dispute. Instead, ex ante investment may simply be ex ante waste, as no amount of preparation may be able to help parties reduce the potential later costs of national security intervention. And CFIUS is not the only review process that muddies the trade-off: The United States' active exporting of CFIUS-like processes to allies means that cross-border deals may face regulatory uncertainty from other countries' review processes as well.

III. PRACTICAL IMPLICATIONS FOR FURTHER RESEARCH

Thus far, this Essay has focused on a descriptive account of national security creep and a discussion of its theoretical implications. But national security creep also has practical import. This Part highlights some of the most salient practical implications, inviting further research on these and other questions raised by this Essay's account of national security creep.

---

271. Jalinous et al., CFIUS Outreach on Non-Notified Transactions, supra note 8.

272. Id.

273. See CFIUS Overview: Committee on Foreign Investment in the United States, Cooley LLP, https://www.cooley.com/services/practice/export-controls-economic-sanctions/cfius-overview [https://perma.cc/699V-HUJ6] (last visited Oct. 6, 2022) (noting that "[a]bsent a voluntary filing, CFIUS may unilaterally initiate a review of a covered transaction at any time, including after the transaction has closed").

274. Jalinous et al., CFIUS Outreach on Non-Notified Transactions, supra note 8.

A. *Nationalism and Blowback in Investment Processes*

Diffusion of CFIUS-like processes may heighten the risk of nationalism in investment screening decisions and of blowback for investors from some countries, including the United States, that attempt to invest abroad. CFIUS has long used a risk-based analysis to evaluate transactions,[275] and the "threat" portion of that analysis has been understood to vary based on the country involved in a transaction.[276] But country-based differential treatment in national security reviews is becoming more overt.

In amending the CFIUS statute in 2018, Congress considered requiring but ultimately declined to require heightened scrutiny for investments from particular countries.[277] Nonetheless, FIRRMA explicitly contemplates differential treatment for investors from certain countries, with some receiving benefits and others greater scrutiny. On the benefit side, FIRRMA authorizes CFIUS to grant preferential treatment to investors from "excepted foreign states"—a list that the Treasury Department has so far determined to include Australia, Canada, New Zealand, and the United Kingdom.[278] But on the opposite end of the spectrum, FIRRMA also specified that CFIUS may consider "whether a covered transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security."[279] That factor clearly references China, and as discussed above, the extant restrictions on outbound investment explicitly target companies linked to China's military.[280]

The risks of blowback come in at least two varieties. First, it is not at all clear that the United States, in encouraging the establishment of CFIUS-like national security reviews among allies, has fully considered the risks of those processes being used against U.S. investors—or that U.S. companies have.[281] In issuing its investment screening regulation, the European Commission emphasized that while "[n]o specific third country

275. See supra notes 58–59 and accompanying text.

276. See, e.g., Farhad Jalinous, Karalyn Mildorf & Keith Schomig, National Security Reviews 2018: United States, White & Case LLP (Nov. 15, 2018), https://www.whitecase.com/insight-our-thinking/national-security-reviews-2018-united-states [https://perma.cc/43CY-F9UR] (noting "rising sensitivity to China-based transactions," which CFIUS subjects to "significant scrutiny").

277. Cathleen D. Cimino-Isaacs & James K. Jackson, Cong. Rsch. Serv., IF11334, CFIUS: New Foreign Investment Review Regulations 2 (2020), https://sgp.fas.org/crs/natsec/IF11334.pdf [https://perma.cc/7LZN-RYPP].

278. See supra notes 95–101 and accompanying text (discussing excepted foreign states).

279. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1702(c)(1), 132 Stat. 1653, 2176 (2018).

280. See supra notes 149–164 and accompanying text.

281. Cf. Schmidt et al., supra note 11 (noting U.K. government scrutiny of transactions involving U.S. parties and warning U.S. and other non-U.K. investors to consider any potential U.K. nexus for their transactions).

is 'targeted'[,] [c]oncerns relating to security and public order can potentially arise from anywhere."[282]

Despite generally strong alliances between the United States and Western Europe, European countries do regard the United States as a security risk in some sense. U.S.–European relations have repeatedly become strained over allegations of U.S. espionage.[283] The U.S. government has in the past solicited and even compelled U.S. companies to assist in serving national security goals.[284] In other instances, assistance by U.S. companies has been unknowing. For example, the Snowden disclosures revealed that the National Security Agency (NSA) "secretly broke[] into the main communications links that connect Yahoo and Google data centers around the world," allowing the NSA "to collect at will from hundreds of millions of user accounts."[285]

Given this history, one could imagine that in a future period of strained U.S.–European relations, E.U. countries doing a risk assessment with respect to a U.S. investor might perceive an undesirable level of threat due to an investor's relationship, whether witting or unwitting, with the

---

282. Eur. Comm'n, FAQs, supra note 110, § I.4.

283. See Stephen Castle, Report of U.S. Spying Angers European Allies, N.Y. Times (June 30, 2013), https://www.nytimes.com/2013/07/01/world/europe/europeans-angered-by-report-of-us-spying.html (on file with the *Columbia Law Review*) (reporting on allegations, initially published by Der Spiegel, that the United States spied on the European Union); Alison Smale, Anger Growing Among Allies on U.S. Spying, N.Y. Times (Oct. 23, 2013), https://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html (on file with the *Columbia Law Review*) (discussing allegations that the United States spied on French government officials and German Chancellor Angela Merkel). See generally Kristina Daugirdas & Julian Davis Mortenson, In Wake of Espionage Revelations, United States Declines to Reach Comprehensive Intelligence Agreement With Germany, 108 Am. J. Int'l L. 815 (2014) (discussing the aftermath of the Merkel spying allegations); Rym Momtaz & Hans von der Burchard, 'Not Acceptable.' France Asks US, Denmark for Clarity on Spying Allegations, Politico (May 31, 2021), https://www.politico.eu/article/france-asks-us-denmark-to-clarify-spying-practices/ [https://perma.cc/2GSH-YV59] (describing European politicians' reactions to reports that Denmark helped the United States spy on European officials); NSA Spying Row: Denmark Accused of Helping US Spy on European Officials, BBC (May 31, 2021), https://www.bbc.com/news/world-europe-57302806 [https://perma.cc/4VRW-95MP] (same).

284. See, e.g., Kristen E. Eichensehr, Digital Switzerlands, 167 U. Pa. L. Rev. 665, 677–79 (2019) (discussing tech companies' efforts to resist U.S. government demands and gag orders); Jon D. Michaels, All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 Calif. L. Rev. 901, 908–19 (2008) (describing informal collaboration between companies and U.S. intelligence agencies); Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stan. L. Rev. 99, 112–22 (2018) (discussing how tech companies are "surveillance intermediaries" that "stand[] between the government and the target of the surveillance" and can thus resist government demands).

285. Barton Gellman & Ashkan Soltani, NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say, Wash. Post (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (on file with the *Columbia Law Review*).

U.S. government. The very CFIUS-like processes that the U.S. government has encouraged allies to establish could be turned back against U.S. investors.[286]

A second possible version of blowback comes not from U.S. allies but from countries targeted for concern via CFIUS, notably China. As U.S. allies stand up investment reviews with the more-or-less explicit goal of blocking investment from China in particular,[287] the world may move increasingly toward a decoupling of the worldwide economy into economic blocs.[288] China itself restricts foreign investment in certain sectors,[289] but more importantly, one could imagine China pressuring other countries to reject U.S. investment—essentially forcing countries to choose between

---

286. Cf. John Kabealo, The Growing Global Alignment in Regulating Chinese Trade and Investment, Atl. Council: Blogs (June 8, 2021), https://www.atlanticcouncil.org/blogs/the-growing-global-alignment-in-regulating-chinese-trade-and-investment/ [https://perma.cc/FEV8-8BCK] ("We do not currently have a thoughtful policy for dealing with countries that implement FDI screening processes at our urging, but use them to restrict US investment.").

287. For example, although the September 2022 CFIUS executive order does not explicitly mention China, press reports highlighted the order's effects on Chinese investment into the United States. E.g., David E. Sanger, Biden Issues New Order to Block Chinese Investment in Technology in the U.S., N.Y. Times (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/us/politics/biden-china-tech-executive-order.html (on file with the *Columbia Law Review*) (describing the order as "designed to sharpen the federal government's powers to block Chinese investment in technology in the United States and limit its access to private data on citizens").

288. Some amount of decoupling is already underway, particularly in the technology sphere. See, e.g., Jon Bateman, Carnegie Endowment for Int'l Peace, U.S.-China Technological "Decoupling": A Strategy and Policy Framework 1 (2022), https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf [https://perma.cc/R7SK-NK4V] (noting that "[a] partial 'decoupling' of U.S. and Chinese technology ecosystems is well underway" and crediting China as "play[ing] an active role in this process," while "the U.S. government has been a primary driver" (footnote omitted)); David J. Lynch & Ellen Nakashima, Economic Ties With China Take a Backseat to National Security, Wash. Post (Oct. 29, 2022), https://www.washingtonpost.com/us-policy/2022/10/29/china-us-trade-economy-national-security/ (on file with the *Columbia Law Review*) (last updated Oct. 31, 2022) (describing the Biden Administration's export controls on certain semiconductors to China as "the most forceful display yet of the administration's evolving strategy of high-tech containment").

289. China updated its Foreign Investment Law in 2019, with changes effective in 2020, and continues to employ a "negative list management" system to prohibit or restrict foreign investment in certain sectors. China: Foreign Investment Law Passed, Libr. of Cong. (May 30, 2019), https://www.loc.gov/item/global-legal-monitor/2019-05-30/china-foreign-investment-law-passed/ [https://perma.cc/MP4L-6AP4] (providing an overview of the Foreign Investment Law). See generally Mo Zhang, Change of Regulatory Scheme: China's New Foreign Investment Law and Reshaped Legal Landscape, 37 UCLA Pac. Basin L.J. 179 (2020) (discussing the Foreign Investment Law and the changes it made to China's foreign investment regime); Gerry Shih, Amid Skepticism, China Fast-Tracks Foreign Investment Law to Show Goodwill to Washington, Wash. Post (Mar. 15, 2019), https://www.washingtonpost.com/world/asia_pacific/amid-skepticism-china-fast-tracks-foreign-investment-law-to-show-goodwill-to-washington/2019/03/15/9506b31e-4701-11e9-9726-50f151ab44b9_story.html (on file with the *Columbia Law Review*) (noting that the law "open[ed] up more sectors for foreign investment").

Chinese investment and U.S. investment.[290] Moreover, adverse decisions on foreign investment may prompt trade-based retaliation, such as restrictions on imports into China from countries that restrict Chinese investment.[291]

These risks of blowback suggest that the United States must develop a thoughtful strategy in approaching its own national security reviews of investments. Such decisions are not taken in a vacuum, and other countries will learn from them.[292] The questions are what lessons will they draw, and what impact will they have on U.S. entities seeking to invest abroad?

B. *Impacts on Deal Transparency and Securities Disclosure*

Another potential impact of national security creep is on transparency and disclosure surrounding corporate transactions. Public companies are required to file securities disclosures when they enter into material agreements, which include many acquisition agreements.[293] The purpose of the disclosure is to allow investors to make informed investment decisions. Because these disclosures are posted publicly, however, regulators have easy access to these disclosures and can use them to make enforcement decisions.

Already, transaction parties regularly shunt information out of the primary deal documents to avoid regulatory scrutiny. For example, when parties know they might be subject to antitrust review that requires them to divest some assets, the parties might agree ex ante on which party will make the required divestitures.[294] However, having divestiture information in the primary deal documents—either submitted directly to regulators for review or available for easy regulatory review via public securities

---

290. See, e.g., Kabealo, supra note 286 ("US policymakers would be negligent not to anticipate that China will pressure third countries to take a hard stance against US investment, thereby turning the tools we are working to create against us. . . . China's deftness in dangling access to its markets as a reward for favorable policies will make for a lot of hard decisions in third countries.").

291. Cf. China to Halt Key Australian Imports in Sweeping Retaliation, Bloomberg (Nov. 3, 2020), https://www.bloomberg.com/news/articles/2020-11-03/china-to-halt-key-australian-commodity-imports-as-tensions-mount (on file with the *Columbia Law Review*) (reporting Chinese trade restrictions on Australian imports in reaction to, among other things, Australia calling for an "independent probe into the origins of [COVID-19]").

292. Cf. Henry Farrell & Abraham L. Newman, Weaponized Interdependence: How Global Economic Networks Shape State Coercion, 44 Int'l Sec. 42, 76–77 (2019) (discussing how states targeted via "weaponized interdependence" may attempt to insulate themselves against future actions, including by minimizing ongoing interdependence).

293. 17 C.F.R. §§ 229.10–.915 (2021) (requiring a disclosure and description of material contracts).

294. Jeremy McClane, Boilerplate and the Impact of Disclosure in Securities Dealmaking, 72 Vand. L. Rev. 191, 211 (2019) (noting that "[t]he law seeks to ensure that the company discloses enough information to allow investors to make an informed decision about the value of those assets and future prospects, which are inherently difficult to value without detailed information generally only possessed by company insiders").

disclosures—might give regulators advance notice about where the parties think their deal's antitrust issues lie. Because of the fear of tipping off regulators, parties shunt sensitive antitrust information into side letter agreements, thereby sometimes managing to evade regulatory scrutiny.[295]

This hiding of information from antitrust regulators happens against a backdrop of very transparent antitrust regulation. Antitrust regulators post, on an annual basis, detailed information about the types of transactions they will scrutinize.[296] Transactions that do not fall into covered categories will not face antitrust scrutiny, and transactions that do will need to file with the FTC or DOJ prior to closing.[297] Often, antitrust regulators choose not to move forward with a review after a filing—in which case the parties can close the deal without fear of antitrust authorities seeking review later.[298]

In addition, antitrust review is relatively public. With the exception of some sensitive trade information that might be redacted, future deal parties have the benefit of extensive, public precedent about when antitrust regulators act, and how. When parties contest regulators' antitrust decisions, those decisions are litigated publicly and provide additional information for future transactions.[299]

In contrast, there is relatively little guidance for parties on how to deal with the risk of national security review. Because of its sensitive nature, regulators necessarily keep the details of many national security risks under wraps. Filings with CFIUS are confidential, and the Committee does not divulge whether particular transactions are under review, the nature of risks identified with respect to particular transactions or investors, or the contents of mitigation agreements entered into to address national security risks.[300]

But while sensitivity may be necessary, it also creates something of a precedent problem. Deal lawyers rely heavily on precedent when designing deals and drafting contracts. For example, regulatory treatment of an earlier deal might affect how parties design a later deal.[301] In the national

295. Hwang & Jennejohn, supra note 244, at 1295 (noting that side letters "reveal where the contracting parties believe their antitrust issues might lie").

296. See supra note 261 and accompanying text.

297. Hwang, Unbundled Bargains, supra note 27, at 1411 n.33.

298. Id.

299. See, e.g., Edmund Lee & Cecilia King, AT&T Closes Acquisition of Time Warner, N.Y. Times (June 14, 2018), https://www.nytimes.com/2018/06/14/business/media/att-time-warner-injunction.html (on file with the *Columbia Law Review*) (reporting on the completion of the AT&T and Time Warner merger, which had previously been blocked by the DOJ and was finally allowed after a lengthy litigation).

300. U.S. Dep't of the Treasury, CFIUS, supra note 4 (explaining statutorily mandated confidentiality requirements).

301. For example, during the mid-2010s tax inversion wave, deal parties were uncertain about how the Internal Revenue Service (IRS) would treat, for tax purposes, their attempts to reincorporate out of the United States and into lower-tax jurisdictions abroad. In order

security context, secrecy makes precedent hard to come by, at least for parties who are not repeat players or advised by lawyers who are repeat players. This precedential void creates two related potential problems.

First, because national security review is so secretive, parties may see national security review as even more uncertain than other types of review, such as antitrust review. In the face of uncertainty, parties may become even more motivated than usual to avoid putting information into primary deal documents or securities filings, where regulators can find the information and act on it. The result, then, is that over time, regulators may have a harder time regulating, because information about deals is less transparent.

Second, investors and other outsiders have access to less information when parties behave this way. Of course, securities laws require parties to disclose all material information to investors, and companies cannot omit major pieces of information from securities disclosures.[302] There is, however, a fair amount of flexibility in disclosure, which means that parties elect to disclose less information than they otherwise would, thereby depriving investors of significant marginal disclosures.[303] Furthermore, because there is so much uncertainty about what kinds of transactions will be subject to national security review—and when—parties have an incentive to hide information even if they judge that, in the current climate, their deal is unlikely to be subject to review. Fear of post-closing review, which is possible, might motivate many parties to shunt information to private agreements.

Of course, as with any private process, information about the national security review process is obtainable—for the right price. Like other areas of legal practice, some lawyers and advisors are repeat players in the national security review process and can provide private information to their clients about past CFIUS actions and mitigations, for instance. But that information is often proprietary, which brings to the fore familiar concerns about whether access to publicly important information ought to be concentrated in the hands of a select few.[304]

---

to gain more certainty, they relied on precedent transactions and private letter rulings from the IRS. See generally Cathy Hwang, The New Corporate Migration: Tax Diversion Through Inversion, 80 Brook. L. Rev. 807 (2015) (discussing the mid-2010s tax inversion wave, as well as prior waves of inversions and IRS responses).

302. Jeremy R. McClane, The Sum of Its Parts: The Lawyer-Client Relationship in Initial Public Offerings, 84 Fordham L. Rev. 131, 141 (2015) [hereinafter McClane, The Sum of Its Parts] (discussing the challenges of applying the materiality standard in deciding what to include in certain registration statements, since they are both regulatory disclosure and marketing documents).

303. Jeremy McClane, The Agency Costs of Teamwork, 101 Cornell L. Rev. 1229, 1260 (2016) (describing the challenges of determining the right amount of disclosure, given that disclosure affects company value); McClane, The Sum of Its Parts, supra note 302, at 140–41 & n.32 (summarizing SEC-mandated disclosure requirements).

304. For instance, as others have noted, information about deal norms and market terms may already be concentrated in the hands of a few elite firms. Having this market

Further research might consider the right balance between the need for national security sensitivity, on the one hand, and creating the right incentives for future deal parties, on the other. Fixes can come from national security regulators, securities regulators, or investors. National security regulators can create more transparent guidelines about the types of transactions that will be subject to national security review or create an outside date after which closed transactions will not be reviewed retroactively. In the United Kingdom, for instance, regulators can review deals for up to five years post-closing.[305] Securities regulators can create more specific rules about parts of deals that cannot be hidden in side letters.[306] And, finally, investors can work to demand more or better disclosure of deal risks, even those involving national security risk.

C. *Effects on Deal Volume*

The observations in this Essay also set the stage for an important empirical question: What impact will national security creep have on deal volume, both into and out of the United States? For many years, regulatory review of deals for national security reasons was rare, so deal parties could choose either U.S. or non-U.S. deal partners without much consideration of the risk of national security review from U.S. authorities. Recent changes to the CFIUS filing process, increases in CFIUS's interest in various transaction types, and CFIUS's still-tentacular timetable have changed the equation.

In the new regulatory landscape, both inbound and outbound deals involving a U.S. party might be subject to regulatory enforcement—and that enforcement might occur even post-closing, when unwinding the deal becomes a significant cost and challenge.[307]

---

information is, in fact, a way for elite firms to justify their existence and their billing rates. See Elisabeth de Fontenay, Law Firm Selection and the Value of Transactional Lawyering, 41 J. Corp. L. 393, 395–96 (2015) (arguing that the "widening chasm between the most elite corporate law firms and the rest of the pack" stems in part from elite firms' ability to "use their market knowledge to procure better economic deals for their clients"); see also Cathy Hwang, Value Creation by Transactional Associates, 88 Fordham L. Rev. 1649, 1652–55 (2020) (discussing the ways that elite firms add value to corporate transactions). However, concentrating power in the hands of a few elite intermediaries has a variety of shortcomings. See Kathryn Judge, Intermediary Influence, 82 U. Chi. L. Rev. 573, 624–30 (2015) (noting that such "intermediary influence" can lead to market inefficiency, longer intermediation chains, increased market and financial-product complexity, an overly large financial sector, misallocation of capital, and systemic fragility).

305. See supra note 125 and accompanying text.

306. See supra note 257 and accompanying text.

307. See, e.g., J. Tyler McGaughey, CFIUS Is Preparing to Block China From Acquiring Magnachip Semiconductor Corporation, Winston & Strawn LLP: Glob. Trade & Foreign Pol'y Insights (Aug. 31, 2021), https://www.winston.com/en/global-trade-and-foreign-policy-insights/cfius-is-preparing-to-block-china-from-acquiring-magnachip-semiconductor-corporation.html [https://perma.cc/E63B-H37M] (discussing one example of post-closing SEC enforcement); see also supra note 263 and accompanying text.

Even deals that have only nominal U.S. ties might end up within CFIUS's review net. Consider CFIUS's 2021 request for a filing related to a Chinese private equity company's purchase of South Korea's Magnachip, discussed above.[308] The deal parties had not filed voluntarily for CFIUS review, nor did any regulations suggest that they needed to file for mandatory review: Neither party had strong ties to the United States, so they presumably believed that CFIUS did not have jurisdiction over the transaction.[309] In particular, Magnachip has little physical presence in the United States, as all of its manufacturing, research, and development occurs abroad; it has no employees or tangible assets in the United States; it has no sales operations in the United States; and all of its intellectual property is owned by non-U.S. companies.[310] Still, CFIUS asserted jurisdiction and refused to approve the transaction,[311] apparently hinging its jurisdiction on Magnachip's Delaware incorporation, New York Stock Exchange listing, and the fact that the company has a Delaware subsidiary.[312]

Intuitively, it would make sense that increased regulatory costs of this type would chill deal volume for deals involving U.S. parties. Such a chilling effect is not necessarily a bad thing: If the regulatory scrutiny chills deals that would raise legitimate national security concerns, then up-front deal avoidance may be efficient for the deal parties and the government. And importantly, increased regulatory costs might not chill deals entirely. China, for instance, has a notoriously complex regulatory scheme, but deal parties remain interested in investing in and with Chinese counterparties.

The diffusion of CFIUS-like processes outside of the United States raises the likelihood that similar chilling effects might also be diffused

---

308. Chase D. Kaniecki, William S. Dawley & Pete Young, CFIUS Threatens to Block Magnachip Deal; Shows Willingness to Interpret Its Jurisdiction Broadly, Cleary Gottlieb: Cleary Foreign Inv. & Int'l Trade Watch (Sept. 10, 2021), https://www.clearytradewatch.com/2021/09/cfius-threatens-to-block-magnachip-deal-shows-willingness-to-interpret-its-jurisdiction-broadly/ [https://perma.cc/8LT4-WXJQ] (last updated Dec. 15, 2021); see also supra note 269 and accompanying text.

309. Kaniecki et al., supra note 308.

310. Id.

311. See Magnachip Semiconductor Corp., Current Report (Form 8-K) (Dec. 13, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001325702/000119312521355865/d152828d8k.htm [https://perma.cc/4KFB-TT2F] (noting that Magnachip and Wise "have now been advised that CFIUS clearance of the Merger will not be forthcoming and have received permission from CFIUS to withdraw their joint filing"); U.S. Chipmaker Magnachip, China's Wise Road End $1.4 Bln Merger Deal, Reuters (Dec. 13, 2021), https://www.reuters.com/markets/europe/chinas-wise-road-capital-magnachip-call-off-14-billion-deal-2021-12-13/ (on file with the *Columbia Law Review*).

312. Even CFIUS's jurisdictional basis for intervention is shadowy. As law firm Cleary Gottlieb notes, "CFIUS presumably (we say presumably because there is no publicly available explanation from CFIUS regarding its jurisdiction in this case) relied on the fact that Magnachip was a U.S.-listed company incorporated in Delaware with a Delaware subsidiary." Kaniecki et al., supra note 308; see also Van Grack & Brower, supra note 268 (discussing "CFIUS's unprecedented intervention" in the deal).

alongside such processes. The more countries that have robust national security review of inbound investments, the more difficult it becomes for deal parties to choose counterparties in a way that evades scrutiny. Moreover, proliferation of security reviews among countries could actually decrease regulatory friction. For example, one could imagine a beefed-up version of the excepted foreign states process whereby clearance for an investor or deal in one country might be transferrable for that deal or an investors' transactions in another country that is closely allied with the first country.[313]

In short, it is hard to tell, at this point, how national security creep might affect overall deal volume. Instead, an appropriate policy question now is how to balance the goals of open investment and national security—and answering that question is becoming even more urgent in light of governments' conflations of economic and national security.

CONCLUSION

This Essay makes a novel descriptive claim: In recent years, national security review of corporate transactions has "creeped" to claim an ever-larger set of deals as reviewable and even subject to prohibition. Driving national security creep is the U.S. government's increasing conflation of national security and economic security. As the understanding of national security expands, so do the regulatory authorities that the United States and other governments assert to manage it. As we have argued, this national security creep has theoretical implications with respect to judicial deference to the executive branch and scholarly understandings of contract costs, as well as possible practical implications.

But we recognize that our claims are somewhat limited. We don't take a strong normative position on whether national security creep is good or bad, warranted or unwarranted, necessary or perverse, for several reasons.

First, as explained in Part I, conceptions of national security are changing, and there is not agreement outside (or, we suspect, even within) the U.S. government about what national security requires. The concepts of security and national security in particular are certainly broadening, but there is no clear definition of what national security requires or metrics for measuring success. It's difficult to evaluate regulatory processes designed to protect national security when there's a lack of agreement about

313. Some deals trigger investment screening in multiple jurisdictions. See, e.g., Press Release, Viasat, Inc., Viasat and Inmarsat Receive Approval for Proposed Combination From Australia's Foreign Investment Review Board, PR Newswire (Oct. 18, 2022), https://news.viasat.com/newsroom/press-releases/viasat-and-inmarsat-receive-approval-for-proposed-combination-from-australias-foreign-investment-review-board [https://perma.cc/3DAY-ZJLC] (reporting that a proposed merger received clearance from the investment screening mechanisms in the United States, United Kingdom, and Australia).

what exactly the United States is trying to protect—and how. The same is true for other countries that are utilizing CFIUS-like processes.

Second, as highlighted in Part I, much of the substance of and explanations for the national security regulatory processes we have highlighted as ingredients in national security creep are secret. CFIUS and its global counterparts do not disclose publicly, or sometimes even to the regulated parties, the nature of their national security concerns about particular transactions, and there is little by way of public documentation for scholars to review. This secrecy can create ripple effects, potentially driving deal parties to be more secretive about their transactions in order to avoid regulatory scrutiny or to avoid deals that might fall into the regulatory nets altogether.

Third, the regulatory regimes addressed in this Essay are in significant flux. CFIUS's new regulations came into effect in 2020, as did the first U.S. regulations about outbound investment to China. The same is true globally. The United Kingdom's new NSIA just entered into force in January 2022. Simply put, it is early days.

Given these constraints, this Essay aims to begin a conversation about these developments by highlighting their potential domino effects and unintended consequences. It is the first step of a broader conversation and invites policymakers, judges, dealmakers, and other scholars to join the discussion. For each of these audiences, the Essay has suggestions and words of caution.

Executive branch policymakers wield tremendous authority, with only imperfect ex post judicial review. In light of the "regulatory bazooka" nature of CFIUS review, such policymakers should use their authority judiciously. While CFIUS is a trump card that allows the executive to block or unwind deals, doing so can have ripple effects in potentially unanticipated areas, such as investor disclosures and treatment of U.S. investors abroad.

But beyond a plea for executive officials to be careful with their authorities, governments should also be more transparent about how they define national security, what kinds of transactions raise concerns, and why. Greater transparency about what it is that government officials are trying to protect and the nature of the threats to national security they believe they face would bolster the legitimacy of the regulatory regimes discussed above and foster potentially useful contributions and pushback by legislators, judges, scholars, and the public. The Biden Administration's recent CFIUS executive order marks a helpful step toward greater transparency about the nature of the security concerns CFIUS considers—and usefully makes public and explicit considerations that expert CFIUS lawyers have already understood.[314] But the United States and other

314. See, e.g., Brian J. Egan, Michael E. Leiter & Ondrej Chvosta, Executive Order Reinforces CFIUS' Broad Authority to Identify National Security Risks, Skadden, Arps, Slate, Meagher & Flom LLP (Sept. 16, 2022), https://www.skadden.com/insights/publications/

governments can still do more going forward to explain their understanding of and threats to national security to constituencies outside of governments. Certainly, much national security–related information must remain classified, and we are not advocating radical transparency where, for example, all CFIUS filings would be public. Nonetheless, it would be possible, useful, and appropriate for the United States and other governments deploying national security creep to engage in greater public discussions about their theory of national security and the nature of the threats they face. The national security creep–related regulatory regimes appear to be deployed as a broad response to technological competition and data security concerns, but greater transparency about their purpose and effects would enable those outside the executive branch to evaluate—and, if necessary, contest—whether the government's goals are appropriate, whether the regulatory regimes deployed are fit to purpose, and whether the government's efforts are achieving the goal of protecting national security.

Greater transparency about the nature of threats governments are attempting to defend against would also enable better understanding among deal parties and their lawyers about the kinds of transactions that governments are likely to find problematic. That in turn would allow deal parties to structure deals to avoid such concerns and to file when necessary, avoiding post hoc reviews and divestment orders that are hugely disruptive to deal parties and likely suboptimal from the government's perspective as well.

Beyond the executive branch, other actors, inside and outside government, have roles to play with respect to national security creep.

Economically focused national security–related cases may give judges a greater role to play on national security issues than they traditionally have had. Judges may see more cases challenging the government's broad assertions of national security, and while recognizing the government's legitimate security interests, judges are well positioned to provide at least some outside oversight of such claims. Revealing classified information to judges in camera is a well-established process in the United States, and one that could be used to provide some external verification of executive claims and a check on executive branch actions.

2022/09/executive-order-reinforces-cfiuss-broad-authority [https://perma.cc/5LUF-97J8] (noting that the executive order does not "materially change the factors CFIUS regularly considers (or has considered over the past several years)"); President Biden Issues Executive Order Directing CFIUS to Consider Specific Areas of Risk in Reviewing Transactions, Covington & Burling LLP (Sept. 15, 2022), https://www.cov.com/en/news-and-insights/insights/2022/09/president-biden-issues-executive-order-directing-cfius-to-consider-specific-areas-of-risk-in-reviewing-transactions [https://perma.cc/A8T5-QSAX] (noting that the order "highlights to a broader public audience the specific areas on which the Biden Administration and CFIUS are currently focused, which . . . CFIUS itself already has been assessing as a regular part of its reviews for a number of years").

For Congress, the short-term lesson from national security creep may be that it has done enough, at least for now. FIRRMA set in motion expansion of CFIUS's authority and encouraged diffusion of CFIUS-like processes among allies. Although Congress is often eager for CFIUS to do more, for now, CFIUS may be doing enough. With respect to the outbound CFIUS proposals now before Congress, legislators should foster public discussion and transparency about the purpose of restricting outbound investment. Congress can push the executive and make its own contributions to sparking public debate about the metes and bounds of what counts as national security and about how best to protect whatever fits within the definition.

For deal parties, national security creep brings to light practical concerns. Regulatory issues have always introduced risk to deals, and managing regulatory risk is an important part of a deal lawyer's job. National security creep, however, has rendered some of that regulatory risk much harder to manage: Not only is the risk profile constantly changing, but there is little precedent on which to rely. More than ever, dealmakers need to think about how to divide risk between parties when that risk is extremely hard to quantify.

Finally, although this is a challenging area of study, we hope that more scholars from different countries and disciplines will weigh in as national security creep continues. As we have highlighted in prior Parts, the national security review process brings forward a variety of questions, both normative and empirical, and we hope that this Essay serves as a starting point for exploring those interests.