National Security Creep in Corporate Transactions

By

Kristen Eichensehr
University of Virginia School of Law

Cathy Hwang
University of Virginia School of Law

National Security Creep in Corporate Transactions

123 Colum. L. Rev. __ (forthcoming 2023)

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 U.S. Committee on Foreign Investment in the United States (CFIUS), the diffusion of CFIUS-like processes to U.S. allies, 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 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.

[*] Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor, 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 Ashley Deeks, David Fagan, Jill E. Fisch, Larry Fullerton, Jack Goldsmith, John Harrison, Michael Livermore, Paul Mahoney, Thomas Nachbar, Richard Re, Sam Rascoff, Paul Schwartz, and David Zaring, as well as participants in workshops at the Council on Foreign Relations, Harvard-Yale-Stanford Junior Faculty Forum, Temple University Beasley School of Law, University of Georgia School of Law, University of Iowa College of Law, University of Pennsylvania Carey Law School, University of Virginia School of Law, and University of Minnesota Law School. Thanks to Sean Michael Blochberger, Lauren Burns, Joshua Goland, Hannah Keefer, Melissa Privette, Dev Ranjan, and Divya Vijay for excellent research assistance.

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 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

---

[1] James Griffin, Gay Dating App Grindr is the Latest Victim of US-China Tensions, N.Y. Times (May 15, 2019), https://www.cnn.com/2019/05/14/tech/grindr-china-us-security/index.html (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 et al., CFIUS Blocks Joint Venture Outside the United States, 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/ (noting that CFIUS had blocked a robotics joint venture in China between a U.S. manufacturing company and two U.S. joint venture partners).

[3] Jeanne Whalen & Ellen Nakashima, Biden Expands Trump Order 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/.

[4] U.S. Dep't of Treasury, The Committee on Foreign Investment in the United States (CFIUS), https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

[5] David T. Zaring, CFIUS as a Congressional Notification Service, 83 S. Cal. L. Rev. 81, 87 (2009) (noting that when this article was written, "the Committee itself almost never actually prevents foreign acquisitions from going forward" and that "CFIUS has launched in-depth reviews of acquisitions in thirty-seven of the 1800-plus filings made since 1998").

[6] David Mortlock et al., CFIUS Annual Report Reveals Key Trends in Review of Foreign Investment, Willkie Farr & Gallagher LLP (Aug. 19, 2021), https://www.willkie.com/-

increasing, pushed along by a major congressional expansion of its jurisdiction in 2018.[7]

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 has always been cloaked in secrecy.[10] *Bloomberg* recently wished "[g]ood luck" to those seeking to understand CFIUS's work, noting that

---

/media/files/publications/2021/08/cfiusannualreportrevealskeytrendsinreviews.pdf (noting that CFIUS reviewed 313 covered transactions in 2020 and that "CFIUS has stepped up its scrutiny of transactions that were not brought to the Committee's attention").

[7] See infra notes 81-100 and accompanying text.

[8] See, e.g., Covington & Burling LLP, CFIUS in the Biden Administration (Jan. 29, 2021), https://www.cov.com/en/news-and-insights/insights/2021/01/cfius-in-the-biden-administration (predicting how the Biden Administration will use the CFIUS review process); Farhad Jalinous et al., White & Case LLP, CFIUS Outreach on Non-Notified Transactions: What it Means, What to Expect, and How to Successfully Navigate the Process (June 1, 2021), https://www.whitecase.com/publications/alert/cfius-outreach-non-notified-transactions-what-it-means-what-expect-and-how (noting that FIRRMA's passage resulted in a "significant increase in resource allocated [to CFIUS] for monitoring and enforcement and the establishment of a formal process to identify so-called 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); 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 Article addresses. See infra note 49.

[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. Dept. of the Treasury, The Committee on Foreign Investment in the United States, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited July 30, 2022) (noting that "Section 721 of the Defense Production Act of 1950 . . . mandates confidentiality protections with respect to information filed with the Committee" and that "Consistent with section 721, the Committee does not publicly confirm or deny that a transaction has been notified to CFIUS"); Verstein, supra note 5, at 775 (discussing national security review—especially under FOCI—as "secretive").

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 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

[11] David McLaughlin, Saleha Mohsin & Jacob Rund, All about CFIUS, Trump's Watchdog on China Dealmaking, Bloomberg (Sept. 15, 2020), https://www.bloomberg.com/news/articles/2018-03-23/all-about-cfius-trump-s-watchdog-on-china-dealmaking-quicktake.

[12] Kevin Granville, CFIUS, Powerful and Unseen, Is a Gatekeeper on Major Deals, N.Y. Times (Mar. 8. 2018), https://www.nytimes.com/2018/03/05/business/what-is-cfius.html.

[13] Fairchild Semiconductor called off the transaction in 1987, "reportedly 'bowing to intense pressure from Reagan Administration officials.'" Analysis: Semiconductors Made CFIUS, Bloomberg Law (June 12, 2020), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-semiconductors-made-cfius (describing the semiconductor industry as one that has always particularly interested national security regulators); see also Chris Miller, A Semiconducted Trade War, For. Pol'y (July 1, 2019), https://foreignpolicy.com/2019/07/01/a-semiconducted-trade-war/ (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 (Jul. 8, 2021), https://www.law.com/2021/07/08/commercial-leases-and-other-real-estate-transactions-are-subject-to-national-security-review/?slreturn=20210912154440 (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 (Feb. 14, 2020), available https://sgp.fas.org/crs/natsec/RL33388.pdf (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").

indirect or non-controlling—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 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* investments. 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

---

[16] See infra notes 85-88 and accompanying text.

[17] See infra section II.B.

[18] See infra section I.B.2.

[19] See infra notes 141-156 and accompanying text.

[20] 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/.

[21] See infra notes 157-167 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 and rationales for such deference. See, e.g., Curtis A. Bradley, Chevron Deference and Foreign Affairs, 86 Va. L. Rev. 549 (2000); 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, Foreign Sovereigns as Friends of the Court, 102 Va. L.

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 the scope of the national security claims. But there is 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

---

Rev. 289 (2016); Kristen E. Eichensehr, Courts, Congress, and the Conduct of Foreign Relations, 85 U. Chi. L. Rev. 609 (2018); 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, Chevronizing Foreign Relations Law, 116 Yale L.J. 1170, 1203, 1205 (2007).

[23] See infra Section II.A.1.

[24] See infra section II.A.1.

[25] Id.

[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., Cathy Hwang, Unbundled Bargains: Multi-Agreement Dealmaking in Complex Mergers & Acquisitions, 164 U. Pa. L. Rev. 1403 (2016) (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 (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 Western L. Rev. 187 (2005) (considering the role of litigation in motivating

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 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 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, Part IV 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 concludes 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

contract design); Albert H. Choi & George G. Triantis, Strategic Vagueness in Contract Design: The Case of Corporate Acquisitions, 119 Yale L.J. 848 (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).

[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) ("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.").

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 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 the expansion of national security, 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.

---

[29] Office of the Dir. of Nat'l Intell., Annual Threat Assessment of the U.S. Intelligence Community (Feb. 2022), available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf (capitalization omitted).

[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 et al., Toward a Geoeconomic Order in International Trade and Investment, 22 J. Int'l Econ. L. 655, 665 (2019) (arguing that "[t]reating economic security as national security may also create a permanent state of exception justifying broad protection/protectionist measures across time and space" 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").

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 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 and her coauthors 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

---

[32] White House, National Security Strategy of the United States of America 14 (Dec. 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[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 (chronicling Trump administration invocations of national security for economic actions).

[34] President Joseph R. Biden, Jr., White House, Interim National Security Strategic Guidance 15 (Mar. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf; see also id. at 22 (calling "traditional distinctions between foreign and domestic policy—and among national security, economic security, health security, and environmental security . . . less meaningful than ever before").

[35] Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, The Geoeconomic World Order, Lawfare (Nov. 19, 2018, 11:17 AM), https://www.lawfareblog.com/geoeconomic-world-order.

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

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 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 does not trust the Chinese government with sensitive personal data of the type that might be shared via a dating app.[42] Social media apps implicate national security too: The Trump administration sought to ban TikTok and other Chinese-owned apps due to national security concerns,[43] and concerns persist about access from China to the data of U.S. TikTok

---

[37] Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, Geoeconomics: The Variable Relationship Between Economics and Security, Lawfare (Nov. 27, 2018, 7:00 AM), https://www.lawfareblog.com/geoeconomics-variable-relationship-between-economics-and-security.

[38] Id.

[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, 1032-44 (2020).

[40] Heath, supra note 39, at 1080-81; see also Heath, supra note 28, at 328-31 (discussing recent World Trade Organization panel decisions about national security exceptions).

[41] Griffiths, supra note 1.

[42] Id.

[43] Kristen Eichensehr, United States Pursues Regulatory Actions Against TikTok and WeChat over Data Security Concerns, 115 Am. J. Int'l L. 124 (2021); 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/ (reporting that divestment negotiations are continuing in the Biden administration).

users.[44] Secretary of State Antony Blinken recently signaled that the broad approach will continue, explaining 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."[45]

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. presidents to deploy a variety of regulatory tools, like CFIUS reviews, economic sanctions, and export controls,[46] 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.[47]

---

[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.

[45] Antony J. Blinken, Secretary of State, 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/; 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.").

[46] See U.S. Dep't of the Treasury, Sanctions Programs and Country Information, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information (last visited July 30, 2022) (listing sanctions programs); U.S. Dep't of Commerce, Bureau of Industry & Security, Recently Published Regulations, https://www.bis.doc.gov/index.php/regulations (last visited July 30, 2022) (collecting export control regulations); U.S. Dep't of State, Directorate of Defense Trade Controls, Learn about Export Regulations, https://www.pmddtc.state.gov/ddtc_public (last visited July 30, 2022) (providing information on export of defense trade items).

[47] 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/ (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.[48] 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, we address three major recent developments with respect to investment reviews that contribute to national security creep: the expansion of the scope of CFIUS's

[48] 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 "the Departments of Defense, Homeland Security, and Justice (informally known as 'Team Telecom')." Ryan Brady & Farhad Jalinous, Team Telecom Two-Year Anniversary, JD Supra (Apr. 26, 2022). 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). 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 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 In the Matter of Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, FCC 20-133 (Sept. 20, 2020), https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf. 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." Sidley, FCC Standardizes and Formalizes "Team Telecom" Review (Jan. 27, 2021), https://www.sidley.com/en/insights/newsupdates/2021/01/fcc-standardizes-and-formalizes-team-telecom-review. The Team Telecom process shares some similarities with the CFIUS process and a single transaction can be subject to review via both processes. Id. 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 Brady & Jalinous, 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.

review, the diffusion of CFIUS-like processes to other countries, and new regulations that restrict outbound transactions.

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, [49] the scope of the Committee's authority has increased dramatically in recent years, so much so as to be nearly unrecognizable from earlier accounts. This section provides an in-depth account of CFIUS's process and scope as it currently operates.

---

[49] In the last decade or so, a few major articles have addressed national security reviews. Given the major changes that have occurred in the last two years, however, none reflect the current scope of or procedures for such processes. In a 2009 article, David Zaring made the novel argument that CFIUS functions primarily as a "congressional notification service." Zaring, supra note 5. But when Zaring wrote, CFIUS was far less active than it is today and, as Zaring noted, "almost never actually prevent[ed] foreign transactions from going forward." Id. at 87. The CFIUS of a dozen years ago and today's CFIUS are so different as to be almost entirely different entities. Jon Michaels' more recent 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, supra note 9, at 807-08. The third paper on national security review of deals is also the one that deals with CFIUS most tangentially. Andrew Verstein's 2017 article mentions CFIUS, but focuses on government intervention in defense companies operated under foreign ownership, control or influence (FOCI). Verstein, supra note 9. 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. Id. at 795. Verstein's paper, however, focuses almost entirely on the FOCI process, mentioning CFIUS only briefly.

A major federal court case, discussed infra notes 196-204 and accompanying text, also prompted a small bumper crop of student notes. See, e.g., Hunter Deely, 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 Protections of Investors' Constitutional Rights Against Government's National Security Review, 15 J. Int'l Bus. & L. 361 (2015).

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

a. The CFIUS Process

CFIUS is an interagency committee chaired by the Secretary of the Treasury and including 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 & Technology Policy.[50] The Director of National Intelligence and Secretary of Labor serve as *ex officio* non-voting members of the Committee.[51] In its current structure, CFIUS reviews voluntary and some mandatory filings by parties to transactions that may pose national security concerns.[52]

CFIUS screens transactions using a multi-step process.[53] In practice, deal parties often begin the process with a "step zero," in which they informally consult CFIUS before filing formally.[54] The official CFIUS process begins when transaction parties file either a short-form declaration or a formal written notice.[55] The filing of a written notice (whether done initially or upon CFIUS's request after the filing of a short-form declaration) triggers a 45-day review period during which CFIUS conducts a risk assessment to determine whether the transaction threatens to impair U.S. national security.[56] 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."[57] 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 45-day national security investigation (subject to a possible 15-day extension).[58]

---

[50] U.S. Dep't of Treasury, CFIUS Overview, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview.

[51] Id.

[52] As discussed below, Congress required mandatory filings in the 2018 FIRRMA legislation. See infra notes 89-92 and accompanying text.

[53] See generally 31 C.F.R. Part 800.

[54] See Cong. Res. Serv., supra note 15, at 15-16 (discussing informal consultation process).

[55] See U.S. Dep't of Treasury, supra note 50; Cong. Res. Serv., supra note 15, at 16.

[56] 31 C.F.R. § 800.102, 800.501-.506.

[57] 31 C.F.R. § 800.102.

[58] Cong. Res. Serv., supra note 15, at 20; 31 C.F.R. § 800.505-.508.

To address identified national security risks, CFIUS may negotiate with transaction parties and conclude agreements to mitigate risks.[59] Such mitigation agreements can include a variety of requirements, such as 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 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."[60] In 2020, approximately 12 percent of notices filed with CFIUS resulted in mitigation agreements, and for each, a CFIUS agency monitors ongoing compliance.[61]

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.[62] The President has 15 days to determine whether to act.[63] 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

---

[59] See Michaels, 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 in order 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 Cong. Res. Serv., supra note 15, at 20.

[60] Comm. on Foreign Investment in the United States, Annual Report to Congress CY 2020, at 40-41, available at https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2020.pdf [hereinafter CFIUS 2020 Rep.]; 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").

[61] CFIUS 2020 Rep., supra note 60, 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.").

[62] Cong. Res. Serv., supra note 15, at 21-22; 31 C.F.R. § 800.508.

[63] 50 U.S.C. § 4565(d)(2).

authority for the President to protect the national security in the matter before the President."[64]

Congress provided a non-exhaustive 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.[65] 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 existence of a threat to national security are not subject to judicial review.[66] To date, Presidents have blocked seven transactions,[67] including ordering ByteDance, the parent company of TikTok, to divest itself of Musical.ly.[68]

Although President Ford initially established CFIUS via executive order in 1975,[69] Congress has codified and repeatedly expanded the authority of the President and CFIUS to review and block transactions on national security grounds.[70] 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.[71] 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.[72]

---

[64] Id. § 4565(d)(2), (4).

[65] Id. § 4565(f).

[66] 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 195-204 and accompanying text (discussing the Ralls case).

[67] Cong. Res. Serv., supra note 15, at 21 (listing five blocked transactions); see also 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, 2021); Executive Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 14, 2020).

[68] Eichensehr, supra note 43; Whalen & Nakashima, supra note 43.

[69] Exec. Order 11,858, 40 Fed. Reg. 20,263 (May 7, 1975).

[70] See, e.g., Zaring, supra note 5, at 91-97 (tracing the evolution of CFIUS through 2009).

[71] Cong. Res. Serv., 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.

[72] Id. at 8-9.

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.[73] Although the criticism eventually prompted Dubai Ports World to sell the U.S. port operations to a U.S. company,[74] 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 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."[75] However, in approving French-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."[76] This and other SSA's "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."[77] 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.[78]

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.[79] 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

---

[73] Id. at 4-5, 9; Michaels, supra note 9.

[74] Cong. Res. Serv., supra note 15, at 4.

[75] Id. at 10; Michaels, supra note 9.

[76] Id. at 9-10.

[77] Id. at 10.

[78] 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.").

[79] For a description of FINSA, see Cong. Res. Serv., supra note 15, at 10-11.

increased congressional oversight through reporting requirements and a requirement that CFIUS member agencies certify to Congress that transactions have no unresolved national security issues.[80]

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).[81] 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."[82]

In FIRRMA, Congress listed 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."[83] Like Congress, the executive branch has expressed concern about risks resulting from foreign governments amassing data on U.S. persons.[84]

---

[80] Id.

[81] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1653, 2174 (Title XVII, Subtitle A); see Cong. Res. Serv., supra note 15, at 11 (noting concerns about "China's growing investment in the United States, particularly in the technology sector").

[82] Pub. L. No. 115-232, Sec. 1702(b)(4), 132 Stat. at 2175.

[83] Id., Sec. 1702(c), 132 Stat. at 2176-77.

[84] 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." U.S. Dep't of Justice, Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-

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.[85] 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) non-controlling '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].[86]

CFIUS review of non-controlling "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

william-p-barr-announces-indictment-four-members-china-s-military; see also id. ("[T]he deliberate, indiscriminate theft of vast amounts of sensitive personal data of civilians, as occurred here, cannot be countenanced."); Eichensehr, supra note 43 at 125-26 (discussing U.S. concerns about TikTok and WeChat collecting large amounts of data from U.S. persons).

[85] 50 U.S.C. § 4565(a)(4). One of us 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. Sec. J. 1 (2022).

[86] U.S. Dep't of Treasury, Proposed Rule, Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. 50,174, 50,174 (Sept. 24, 2019), *available at* https://www.govinfo.gov/content/pkg/FR-2019-09-24/pdf/2019-20099.pdf; *see also* U.S. Dep't of Treasury, Summary of the Foreign Investment Risk Review Modernization Act of 2018, https://home.treasury.gov/system/files/206/Summary-of-FIRRMA.pdf; *see* 50 U.S.C. § 4565(a)(4)(B).

of United States citizens that may be exploited in a manner that threatens national security."[87] CFIUS refers to these as "TID U.S. businesses," standing for "Technology, Infrastructure, and Data."[88]

Mandatory Filing. FIRRMA empowered CFIUS to shift from the voluntary filing system to mandatory filing for certain transactions.[89] 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.[90] 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.[91] 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."[92]

Significantly, the mandatory filing requirements are subject to exceptions, including for certain "excepted foreign states,"[93] 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 interested 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."[94] Ultimately, CFIUS's regulations "do not target any particular country for greater scrutiny," an issue that was "a major topic of congressional debate during consideration of FIRRMA," but they do establish benefits for certain foreign governments,

---

[87] 50 U.S.C. § 4565(a)(4)(B)(iii); Proposed Rule, supra note 86, 84 Fed. Reg. at 50,176

[88] Proposed Rule, supra note 86, 84 Fed. Reg. at 50,176; see also 31 C.F.R. § 800.248 (defining "TID U.S. business").

[89] See 50 U.S.C. § 4565(b)(1)(C)(v)(IV) ("Mandatory declarations"); see also Cong. Res. Serv., supra note 15, at 19 (discussing FIRRMA's provision of authority for mandatory filing).

[90] 31 C.F.R. § 800.401.

[91] Id. § 800.244 (defining "substantial interest").

[92] Id. § 800.901.

[93] See id. § 800.401(b)(1).

[94] NDAA, Sec. 1702(c)(1).

termed "excepted foreign states," and for investors from those countries.[95] 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.[96] The list of excepted foreign states now includes all members of the Five Eyes intelligence sharing alliance (and no other countries).[97]

Going forward, states have to satisfy additional criteria to maintain or obtain excepted status,[98] 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."[99] 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

---

[95] Cong. Res. Serv., supra note 15, at 19; see 31 C.F.R. § 800.218 ("Excepted foreign state"); id. § 800.219 ("Excepted investor").

[96] Dep't of the Treasury, Office of Investment Security, Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112, 3116 (Jan. 17, 2020); see also U.S. Dep't of Treasury, Fact Sheet: Final Regulations Modifying the Definitions of Excepted Foreign State and Excepted Real Estate Foreign State and Related Actions 2-3 (Jan. 5, 2022), https://home.treasury.gov/system/files/206/Fact-Sheet-Final-Rule-Revising-EFS-Definitions-2.pdf (noting the addition of New Zealand); U.S. Dep't of Treasury, CFIUS Excepted Foreign States, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states (showing effective dates of excepted foreign state status).

[97] 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 et al., Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Use about Intelligence-Sharing Arrangements, Lawfare (Apr. 23, 2018), https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing.

[98] See 31 C.F.R. § 800.218, § 800.1001.

[99] Id. § 800.1001; see also U.S. Dep't of Treasury, Factors for Determinations under § 800.1001(a)/§ 802.1001(a), at 1-2, https://home.treasury.gov/system/files/206/Excepted-Foreign-State-Factors-for-Determinations.pdf.

investments.[100] CFIUS has already determined that Australia and Canada meet these criteria and will remain excepted foreign states.[101]

CFIUS's new process to differentiate overtly among foreign countries involved in transactions is a carrot-based approach to encouraging 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.

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.[102] Congress in FIRRMA expressed its sense that 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."[103] 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.[104] Several examples illustrate this trend.

---

[100] U.S. Dep't of Treasury, supra note 99, at 2.

[101] U.S. Dep't of the Treasury, Determination Regarding Excepted Foreign States, 87 Fed. Reg. 731 (Jan. 6, 2022).

[102] See White House, National Strategy for Critical and Emerging Technologies 9 (Oct. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf ("Engage allies and partners to develop their own processes similar to those executed by the Committee on Foreign Investment in the United States (CFIUS)."); see also Thomas Freddo, Will Biden Use Every Tool Against Beijing?, Wall St. J. (Apr. 23, 2021), at A13 (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").

[103] Pub. L. No. 115-232, Sec. 1702(b)(6), 132 Stat. at 2176.

[104] See, e.g., Sarah Bauerle Danzman & Sophie Meunier, The Big Screen: Mapping the Diffusion of Foreign Investment Screening Mechanisms (unpub. manuscript) (2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3913248 (chronicling the recent proliferation of investment screening mechanisms in Organisation for Economic Co-operation and Development countries); James K. Jackson & Cathleen D. Cimino-Isaacs, Cong. Res. Serv., CFIUS Reform Under FIRRMA 2 (Feb. 2, 2020), https://fas.org/sgp/crs/natsec/IF10952.pdf (detailing investment-review-related actions, including blocking of deals, by the European Commission, Canada, the United Kingdom, Germany, and China).

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.[105] Although the regulation 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."[106] 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.[107] 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."[108] The regulation explicitly permits international cooperation, specifying that "Member States and the Commission may cooperate with the

---

[105] Regulation 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investments Into the Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R0452-20200919; id. at art. 17 (specifying that the "Regulation shall apply from 11 October 2020"). "Foreign" for purposes of the regulation means "[c]ases where the acquisition of an EU target involves direct investment by one of more entities established outside the Union." 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 8, C(2020) 1981 final, Mar. 25, 2020, available at https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158676.pdf (emphasis omitted).

[106] Regulation 2019/452, supra note 105, at art. 1.

[107] Id. at art. 6; see also id. at 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. at art. 6(3).

[108] Id. at art. 4.

responsible authorities of third countries on issues relating to the screening of foreign direct investments on grounds of security and public order."[109]

The Commission has encouraged member states to establish or expand FDI screening mechanisms,[110] and a growing number of states have done so.[111] As of October 2020, 15 EU member states had FDI screening mechanisms in place,[112] and by June 2021, the number had increased to 18 states.[113]

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.[114] Touted as "the biggest shake-up in the U.K.'s industrial intervention policy for nearly two decades,"[115] 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, along with government authority to "call-in"

---

[109] Id. at art. 13.

[110] Communication from the Commission, supra note 105, at 2.

[111] See, e.g., Cleary Gottlieb, EU Foreign Direct Investment Regulation Comes into Force, at 4, Oct. 16, 2020, https://www.clearygottlieb.com/-/media/files/alert-memos-2020/eu-foreign-direct-investment-regulation-comes-into-force.pdf ("[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)." (footnote omitted)).

[112] Peter Camesasca et al., 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/.

[113] Eur. Comm'n, Frequently Asked Questions on Regulation 2019/452 Establishing a Framework for the Screening of Foreign Direct Investments into the Union 11 & n.4, available at https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157945.pdf; see also Eur. Comm'n, List of Screening Mechanisms Notified by Member States (last updated July 14, 2021), https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf.

[114] See Covington, UK FDI: National Security & Investment Law Is Approved by Parliament (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. For the full text of the NSIA, see National Security and Investment Act 2021, UK Public General Acts, https://www.legislation.gov.uk/ukpga/2021/25/contents/enacted.

[115] 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.

investments, both within and outside of those sectors, for review of national security risks.[116]

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 Investment Security Unit.[117] 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."[118] 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."[119] 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).[120] The Act carries substantial penalties for noncompliance, including fines, corporate criminal penalties, and up to five years jail time for directors and officers.[121]

Prior to the NSIA, the U.K. 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,[122] but it had intervened for national security reasons only twelve times

---

[116] See Covington, supra note 114 (describing bill); John Schmidt, et al., A New Mandatory UK Foreign Direct Investment Regime Gets Royal Assent: The Five Key Things You Need to Know, Arnold & Porter, May 10, 2021, https://www.arnoldporter.com/en/perspectives/publications/2021/05/a-new-mandatory-uk-fdi-regime-gets-royal-assent.

[117] Covington, supra note 114; Schmidt, supra note 116. For an overview of the process, see Dep't for Business, Energy & Industrial Strategy, Policy Paper: The National Security and Investment (NSI) Regime: Process for Businesses Factsheet (Mar. 3, 2021), https://www.gov.uk/government/publications/national-security-and-investment-bill-2020-factsheets/the-national-security-and-investment-nsi-regime-process-for-businesses-factsheet.

[118] Schmidt, supra note 116.

[119] Dep't for Business, Energy & Industrial Strategy and Rt. Hon. Alok Sharma MP, Press Release, New Powers to Protect UK from Malicious Investment and Strengthen Economic Resilience, Nov. 11, 2020, https://www.gov.uk/government/news/new-powers-to-protect-uk-from-malicious-investment-and-strengthen-economic-resilience.

[120] Covington, supra note 114.

[121] Id.

[122] See, e.g., Linklaters, CFIUK? UK Introduces National Security and Investment Bill (Nov. 11, 2020), https://www.linklaters.com/en/insights/publications/2020/november/cfiuk-uk-

since 2002.[123] The government estimates that the new NSIA will result in 1,000-1,830 notifications per year, with an additional 70-95 investments called in by the government, and remedies imposed in "[a]round 10" cases.[124] In "one of the first major test cases" of the NSIA, the U.K. is reportedly considering whether to unwind the 2021 acquisition of a British computer chip company by a Chinese-controlled company,[125] and in July 2022, the U.K. government used the NSIA authority for the first time to block a transaction.[126]

Australia. After tightening foreign investment review on national security grounds for several years,[127] Australia announced a major reform to its foreign investment review system in June 2020,[128] with the changes effective at the start of 2021.[129] Australia amended its Foreign Acquisitions

---

introduces-national-security-and-investment-bill (discussing Enterprise Act 2002 and history of national security review).

[123] Impact Assessment, National Security and Investment Bill, Sept. 22, 2020, at 11, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf.

[124] Id. at 22.

[125] 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 (discussing review of Nexperia's acquisition of Newport Wafer Fab). U.S. Congressmen have also raised concerns about the acquisition. See Sion Barry, U.S. Congressmen Call for Chinese Takeover of Welsh Tech Firm Newport Wafer Fab to Be Overturned on Security Grounds, BusinessLive (Apr. 21, 2022), https://www.business-live.co.uk/enterprise/congressmen-call-chinese-takeover-welsh-23742183.

[126] U.K. Dep't for Bus., Energy & Indus. Strategy, Publication of Notice of Final Order (July 20, 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092802/aquisition-scamp5-scamp7-know-how-final-order-notice-20220720.pdf (blocking Beijing Infinite Vision Technology Co. Ltd. from acquiring vision sensing technology from the University of Manchester); see also 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.

[127] 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; U.S. Dep't of State, 2020 Investment Climate Statements: Australia, https://www.state.gov/reports/2020-investment-climate-statements/australia/ (discussing changes beginning in 2017).

[128] Hon. Josh Frydenberg MP, Treasurer of the Commonwealth of Australia, Major Reforms to Australia's Foreign Investment Framework (June 5, 2020), https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/major-reforms-australias-foreign-investment-framework.

[129] See Jones Day, Significant Changes to Australia's Foreign Investment Framework Commenced on 1 January 2021, Jan. 2021,

and Takeovers Act 1975 in 2020 to require approval by the Foreign Investment Review Board of foreign persons engaging in "notifiable national security actions," including acquiring interests in national security businesses or land with a connection to national security.[130] "National security businesses" 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.[131] 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.[132] Moreover, the legislation grants the Treasurer a "last resort review power to reassess approved foreign investments where subsequent national security risks emerge" and to "impose conditions, vary existing conditions, or, as a last resort, require the divestment of foreign interests in a business, entity or land."[133] The 2020 legislation significantly increased the penalties for non-compliance with the screening mechanisms, including failing to comply with a requirement to obtain prior approval or breaching conditions of approval.[134]

As in the United States, the reforms appear motivated in large part by Chinese investments.[135] According to research by Australian National

---

https://www.jonesday.com/en/insights/2021/01/significant-changes-to-australias-foreign-investment-framework-commenced-on-1-january-2021.

[130] For an overview of the changes, see Jones Day, supra note 129; for the legislation and accompanying regulations, see Australian Gov't, Foreign Investment Review Bd., Legislation, https://firb.gov.au/general-guidance/legislation.

[131] Jones Day, supra note 129; Australia, Foreign Investment Reform (Protecting Australia's National Security) Regulations 2020 (Dec. 10, 2020), https://www.legislation.gov.au/Details/F2020L01568.

[132] Austrl. Gov't The Treasury, Foreign Investment Reforms 13 (June 2020), https://treasury.gov.au/sites/default/files/2020-06/p2020-87595_0.pdf; see also Jones Day, supra note 129.

[133] Austrl. Gov't The Treasury, supra note 132, at 11 https://treasury.gov.au/sites/default/files/2020-06/p2020-87595_0.pdf; see also Jones Day, supra note 129.

[134] See Austrl. Gov't The Treasury, supra note 132, at 17-18; Jones Day, supra note 129 ("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.").

[135] See, e.g., Alderman, supra note 127 (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 (noting that the Australian government "rejected a

University (ANU), "Chinese investment in Australia peaked at A$16.5 billion in 2016, spanning agriculture, transport, energy utilities, healthcare, mining and property."[136] 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.[137]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.[138] 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.'"[139]

Numerous other countries, including Canada, China, Germany, Japan, and New Zealand, have enacted or strengthened existing national security reviews of foreign investments in recent years.[140] It remains to be

---

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").

[136] 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/.

[137] Id.

[138] 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.

[139] 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 (quoting list of grievances from the Chinese government) (internal quotation marks omitted); see also Karp, supra note 138 (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").

[140] Austrl. Gov't The Treasury, supra note 132, at 3 (summarizing changes to foreign investment screening mechanisms by the United States, European Commission, Japan, China, and New Zealand); Alderman, supra note 127 (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 (describing reforms to tighten national security screening of foreign investments in Germany); Gearoid Reidy & Shoko Oda, Japan Moves to Limit Foreign Investment in Half of Listed Firms, Japan Times (May 11, 2020), https://www.japantimes.co.jp/news/2020/05/11/business/economy-business/japan-

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 potential new restrictions on outbound investment from the United States.

On November 12, 2020, then-President Trump issued Executive Order 13,959 on "Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies."[141] The order explained that "[t]hrough a 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,"[142] 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."[143] This strategy allows China, the order alleged, to "exploit[] United States investors to finance the development and modernization of its military."[144] 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.[145] The order gave U.S. investors until November 2021 to divest from prohibited securities.[146] The companies included in the order came from a list compiled by the Secretary of Defense,[147] and included "prominent Chinese technology, manufacturing and infrastructure companies, such as China Mobile Communications Group, China Telecommunications Corporation, Huawei, Sinochem Group, Hangzhou

limit-foreign-investment-listed-firms/ (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").

141 85 Fed. Reg. 73,185 (Nov. 17, 2020).

142 Id. at 73, 185.

143 Id.

144 Id.

145 Id.

146 Id. at 73, 186.

147 Id.

Hikvision Digital Technology, China Railway Construction Corporation, Inspur Group and Aviation Industry Corporation of China."[148]

After two Chinese companies won preliminary injunctions in federal court in challenges to their inclusion on the Defense Department's list,[149] 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.[150] The new order covers not just Chinese companies supporting the Chinese military, but also threats from "the development or use of Chinese surveillance technology."[151] 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.[152]

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 the United States and our allies."[153] An annex to the order listed 59 entities subject to the investment prohibition.[154] The list includes many, like China Mobile Communications Group, China Telecommunications Corporation, and Huawei, that were on the Trump administration list, but adds new companies

---

[148] 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.

[149] See Karen Freifeld, 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 (reporting preliminary injunctions won by Luokung Technology Corp. and Xiaomi Corp. against their inclusion on the investment ban list).

[150] Exec. Ord. 14,032, Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China, 86 Fed. Reg. 30,145 (June 3, 2021).

[151] Id. at 30,145.

[152] 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.

[153] White House, FACT SHEET: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China (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/.

[154] Annex to Exec. Ord. 14,032, 86 Fed. Reg. 30,148, 30,148-49 (June 3, 2021). For the latest version of the list, see U.S. Dep't of the Treasury, Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List), https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list (last visited July 30, 2022).

and omits others.[155] The Biden administration subsequently added additional companies to the list and is reportedly considering additional restrictions on U.S. investment into Chinese companies that work on artificial intelligence and other technologies that could have military applications.[156]

Congress, too, is considering broader restrictions on outbound investment, specifically establishing an interagency committee colloquially called "outbound CFIUS" or "reverse CFIUS."[157] Congress considered and rejected screening outbound investment in 2018,[158] 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.[159] The CNCC would review

---

[155] For a helpful breakdown of companies that were included in both orders or in only one or the other, see President Biden Revamps Communist Chinese Military Companies (CCMC) Sanctions Program, Paul Weiss (June 7, 2021), https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/president-biden-revamps-communist-chinese-military-companies-ccmc-sanctions-program?id=40293#_ftnref5. Among the companies omitted from the Biden administration list are Luokung Technology Corp. and Xiaomi, see id., the two that had won preliminary injunctions against their inclusion on the Trump administration list, see Freifeld, supra note 149. 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.

[156] U.S. Dep't of Treasury Press Release, 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; 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 (discussing concerns in the Biden administration and possible "narrowly tailored" regulation of outbound investments).

[157] See, e.g., Sarah Bauerle Danzman, Is the US Going to Screen Outbound Investment?, Atl. Council (Jan. 10, 2022), https://www.atlanticcouncil.org/blogs/econographics/is-the-us-going-to-screen-outbound-investment/#_ftnref3 (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 (discussing "reverse CFIUS").

[158] See Shawn Donnan, Senators Ditch Plan to Review US Outbound Investment (May 15, 2018), https://www.ft.com/content/a1fcfeec-57cf-11e8-bdb7-f6677d2e1ce8.

[159] Sen. Bob Casey, Senators Introduced an Amendment to the United States Innovation and Competition Act Currently Under Consideration by the Senate (May 24,

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 pose "unacceptable risk to a national critical capability."[160] Like CFIUS, it would also empower the President to take actions to mitigate risks, up to and including prohibiting transactions or seeking divestment.[161] Per the bill, countries of concern would encompass "foreign adversaries" specified in a separate statute and currently including China, Russia, Iran, North Korea, Cuba, and Venezuela, while entities of concern are those with certain ties to such countries.[162] 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."[163]

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 identified by the CNCC."[164] Although the White House endorsed outbound screening,[165] the outbound screening process was omitted from a compromise China competition bill agreed between the House and Senate in July 2022.[166] Nonetheless, the

---

2021), https://www.casey.senate.gov/news/releases/casey-and-cornyn-release-a-joint-statement-on-national-critical-capabilities-defense-act.

[160] See Sen. Amndt. 1853, Cong. Rec.—Senate, S3269-72, May 20, 2021, https://www.congress.gov/117/crec/2021/05/20/167/88/CREC-2021-05-20-pt1-PgS3202.pdf (defining covered transaction and describing CNCC review).

[161] Id. at S3271 (Sec. 1004).

[162] Id. (Sec. 1001(4), (8)); Mario Mancuso & Luci Hague, What Outbound Investment Review Would Mean for US Cos., Law360 (June 17, 2022), https://www.law360.com/articles/1503969.

[163] Casey, supra note 159.

[164] Senators Introduce Compromise Proposal Regarding Review of Outbound Investment, Sidley Austin LLP (Jun. 23, 2022), https://www.sidley.com/en/insights/publications/2022/06/senators-introduce-compromise-proposal-regarding-review-of-outbound-investment.

[165] 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/ (reporting Biden administration support).

[166] John D. McKinnon, Senate Bill to Boost Chip Production, Advanced Technology Set to Move Ahead, Wall St. J. (July 25, 2022), https://www.wsj.com/articles/senate-bill-to-boost-chip-production-advanced-technology-set-to-move-ahead-11658741402 (noting omission of outbound investment screening).

significant bicameral and bipartisan support the CNCC garnered suggests that Congress may revisit an outbound screening mechanism in the near future.[167]

* * *

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 to add to dealmaking costs, but also provide opportunities for arbitrage and value creation.[168] But as the previous Part discussed, national security-related regulation is different in many ways from other types of regulation, even when it is not "creeping": National security is by necessity sensitive and secretive, contributing to a number of regulatory quirks that other regulations do not have.

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,

---

[167] See, e.g., Revised National Critical Capabilities Defense Act of 2022 Proposes Expansive Outbound Investment Review Regime, Covington (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 (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).

[168] 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).

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 because of 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 be scrupulously monitoring 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 in using those authorities than it would if facing robust critical oversight. In a Madisonian sense, ambitions are not counteracting one another, but fostering one another.[169] 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.[170] 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.[171]

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

---

[169] Federalist 51 (Madison).

[170] 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").

[171] 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 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).

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.[172] 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. 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.[173] But with respect to national security creep, 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.[174]

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 giving the government's view preferential consideration to substantial weight to dispositive acceptance.[175] In foreign affairs cases, courts have deployed

---

[172] See infra notes 219-227 and accompanying text.

[173] 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 lawsuit about U.S. drone strike barred by the political question doctrine).

[174] 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).

[175] See, e.g., Peter L. Strauss, Essay, "Deference" Is Too Confusing—Let's Call Them "Chevron Space" and "Skidmore Weight," 112 Colum L. Rev. 1143, 1145 (2012)

multiple kinds of deference to the executive,[176] and such deference may pose a greater hurdle 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 economic-linked 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 where judges continue on their current trajectory of deference to the executive branch on 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 of national security creep. The courts have long afforded deference to agencies' statutory

("'[D]eference' is a highly variable, if not empty, concept . . . sometimes used in the sense of 'obey' or 'accept,' and sometimes as 'respectfully consider.'").

[176] See Bradley, supra note 22, at 659-63 (identifying "five overlapping categories" of foreign affairs deference); Eichensehr, 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).

interpretations,[177] 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 regulations and interpretation.[178] 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."[179]

Beyond statutory interpretation, courts also routinely defer to the executive branch on factual determinations about foreign relations and national security.[180] Judges rely on functional justifications for such "national

---

[177] See United States v. Mead Corp., 533 U.S. 218, 226-28 (2001); Chevron, U.S.A., Inc. v. Nat. Res. Def. Coun., Inc., 467 U.S. 837, 842-43 (1984); Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944). 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, ___ S. Ct. ___ (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/ (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 non-delegation 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 non-delegation); Paul v. United States, 140 S. Ct. 342 (2019) (Kavanaugh, J., statement respecting the denial of certiorari) (suggesting agreement with Gorsuch's opinion in *Gundy* regarding the non-delegation doctrine). Notably, however, Justices who advocate reinvigorating the non-delegation doctrine have suggested that certain circumstances, including delegations to the executive branch to engage in fact-finding and delegations relating to foreign relations, may continue even as other delegations are narrowed. *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) (considering the foreign relations law implications of reinvigorating the non-delegation doctrine).

[178] 10 U.S.C. § 4565(a); 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).

[179] 50 U.S.C. § 1701(a).

[180] See, e.g., Holder v. Humanitarian Law 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" where

security fact deference,"[181] 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.[182]

The Supreme Court has been particularly deferential in circumstances where *predictive* judgments about national security are involved.[183] 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,

---

"sensitive and weighty interests of national security and foreign affairs" are involved); Jama v. Immigration and Customs Enforcement, 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 Central Intelligence Agency (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" (emphasis in original)); Bradley, 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).

[181] 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").

[182] See, e.g., Holder v. Humanitarian Law Project, 561 U.S. 1, 34 (2010) (explaining the Court's deference to factual assessments by the executive about terrorism on the grounds that "[w]e have noted 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'" (quoting Boumediene v. Bush, 553 U.S. 723, 797 (2008)), and that "when it comes to collecting evidence and drawing factual inferences in this area, 'the lack of competence on the part of the courts is marked'" (quoting Rostker v. Goldberg, 452 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").

[183] Bradley, supra note 22, at 661-62 (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 ("Expertise 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, 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." [184] 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."[185] 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. Some judges might well defer to national security claims based on their approach to executive power, perception of the reasonableness of the claims, and 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.[186] In that circumstance, executive branch claims that Chinese companies' access to sensitive personal data or technologies must be restricted to protect national security could find a deferentially disposed audience in the judiciary.[187]

---

[184] 484 U.S. 518, 528-29 (1988).

[185] Id. at 529.

[186] 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; Michèle A. Flournoy, America's Military Risks Losing Its Edge, For. Aff. 76-90 (May/June 2021), https://www.foreignaffairs.com/articles/united-states/2021-04-20/flournoy-americas-military-risks-losing-its-edge; 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; 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/.

[187] Cf. Curtis A. Bradley, Foreign Relations Law and the Purported Shift Away from "Exceptionalism", 128 Harv. L. Rev. F. 294, 303 (2015) ("[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.").

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 what the kinds of cases 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.[188] Similarly, companies subject to claims of jurisdiction by U.S. regulators that are aggressive in scope not because of a company's line of business but because of its limited ties to the United States might contest U.S. jurisdiction.[189] 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 fall 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.[190] WeChat users and TikTok users and content creators sued to challenge the orders, citing both statutory and constitutional claims, including First and Fifth Amendment protections.[191] And TikTok's parent company argued that the statutory exemptions in IEEPA for "information materials" and "personal communication" rendered the administration's actions

[188] See infra notes 207-217 and accompanying text (discussing successful challenges by Xiaomi and Luokung to their designation as companies affiliated with China's military).

[189] Cf. infra notes 289-293 (discussing CFIUS review of the Magnachip deal).

[190] For a description of the orders and resulting litigation, see Eichensehr, supra note 43.

[191] See id. at 126-29 (describing litigation over the TikTok and WeChat bans).

impermissible.[192] The lawsuits resulted in multiple preliminary injunctions against the government from several district courts across the country.[193]

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 the 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,"[194] 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 judge 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, than claims related to, for example, terrorism, which are easier to articulate to judges.

The third possibility noted above—*bifurcation*—also posits a change in judges' willingness to defer, but instead of decreased deference across the board, it instead 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 or classification of national security-related claims wherein they treat executive assertions regarding more traditional national security issues with more deference than newer sort of assertions about the necessity of national

---

[192] Id. at 127-28 (discussing lawsuit by TikTok parent company ByteDance).

[193] See id. at 126-29 (describing preliminary injunctions); see also Order Granting Motion for Preliminary Injunction, U.S. WeChat Users Alliance et al. v. Trump et al., No. 3:20-cv-05910 (N.D. Cal. Sept. 19, 2020) (Doc. 59); Op., TikTok Inc. et al. v. Trump et al., No. 1:20-cv-02658, slip op. at 1 (D.D.C. Sept. 27, 2020) (Doc. 30). Op., TikTok Inc. et al. v. Trump et al., No. 1:20-cv-02658, slip op. at 1, 21, 29 (D.D.C. Dec. 7, 2020) (Doc. 60); Op., Marland et al. v. Trump et al., No. 2:20-cv-04597, slip op. at 28 (E.D. Pa. Oct. 30, 2020) (Doc. 35).

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

security-related restrictions on economic activity. This alternative avoids increasing 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 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, as a descriptive matter, some evidence suggests that judges are pushing back against the government's economically focused national security claims both in the CFIUS context and with respect to outbound investment restrictions.

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."[195] Ralls Corp., 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 threat.[196] CFIUS disagreed.[197] The President ordered the transaction prohibited, and since it had already closed, required Ralls to divest itself of the acquired companies.[198] Ralls sued CFIUS and the President, arguing, among other claims, that the mitigation measures CFIUS had ordered and the divestment order violated

[195] 50 U.S.C. § 4565(e)(1); see also id. § 4565(d)(1), (4).

[196] Ralls Corp. v. Comm. on For. Investment in the U.S., 758 F.3d 296, 305-06 (D.C. Cir. 2014).

[197] Id.

[198] Id. at 306.

the Administrative Procedure Act (APA) and the company's Fifth Amendment due process rights.[199] After rejecting the government's argument that the case presented a political question,[200] 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.[201] Citing the Supreme Court's decision in *Mathews v. Eldridge*,[202] 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."[203] 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 our uncertainty that more process would have led to a different presidential decision."[204]

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*.[205] TikTok's case remains pending, but is currently being held in abeyance at the parties' request.[206]

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 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

---

[199] Id.

[200] Id. at 313.

[201] 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.").

[202] *Ralls Corp.*, 758 F.3d at 317-18 (quoting Mathews v. Eldridge, 424 U.S. 319 (1976)).

[203] Id. at 319.

[204] 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. (Nov. 4, 2015), https://www.wsj.com/articles/BL-252B-8621.

[205] Petn. for Review, TikTok Inc. v. Comm. on Foreign Investment in the United States, No. 20-1444 (D.C. Cir. Nov. 10, 2020).

[206] Order, TikTok Inc. v. Comm. on Foreign Investment in the United States, No. 20-1444 (D.C. Cir. Feb. 19, 2021).

from investing. The first case was brought by Xiaomi Corporation, a "multinational consumer electronics corporation" that produces smartphones, TVs, and laptops.[207] While recognizing that courts generally afford agencies heighted deference in national security-related matters,[208] the court nonetheless concluded that DOD's designation of Xiaomi violated the APA due to inadequate explanation and lack of "substantial evidence," among other issues.[209] 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."[210]

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." [211] Although noting that courts "afford heightened deference to an agency's determination when it concerns national security,"[212] the judge determined that Luokung had shown a likelihood of success on the merits.[213] The district court rejected DOD's broad interpretation of the language defining companies that could be designated,[214] 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.[215] Citing DOD's reliance on "a handful of innocuous facts gathered from company press releases, not any classified security intelligence" 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."[216] Although the judge did not reach Luokung's constitutional procedural due

---

[207] Mem. Op. at 3, Xiaomi Corp. v. U.S. Dep't of Def., No. 21-280 (D.D.C. Mar. 12, 2021) (Doc. 21), available at https://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2021cv00280/226816/21/.

[208] Id. at 8.

[209] Id. at 8-9.

[210] Id. at 25.

[211] Mem. Op. at 4, Luokung Tech. Corp. v. Dep't of Def., No. 21-583 (D.D.C. May 5, 2021) (Doc. 33).

[212] Id. at 9.

[213] Id. at 1.

[214] Id. at 11-18.

[215] Id. at 19-24.

[216] Id. at 31.

process claim, he went out of his way to note that Luokung "raise[s] serious concerns" about due process and "[s]uffice it to say 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."[217]

When combined with the several preliminary injunctions issued against the executive for its actions against TikTok,[218] 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 Curtis Bradley,[219] 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."[220] 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 political question, to preclude judicial review of the merits of such cases.[221] 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.[222] They described the rise of foreign relations exceptionalism in the early twentieth century and

---

[217] Id. at 25 n.13; see also id. at 28 (noting that Luokung shares only trade on Nasdaq).

[218] See supra notes 190-193 and accompanying text.

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

[220] Sitaraman & Wuerth, supra note 194, at 1907-08.

[221] 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).

[222] Id. at 1907-08.

its subsequent dominance through the end of the Cold War, 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.[223] Although Sitaraman and Wuerth endorsed normalization as a normative matter,[224] their arguments prompted significant pushback. Bradley and Carlos Vázquez questioned the descriptive claims about a trend toward normalization in the Supreme Court precedents Sitaraman and Wuerth cite.[225] Bradley and 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.[226] 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."[227]

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 prompts 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 the 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 traditional national security claims.

---

[223] Sitaraman & Wuerth, supra note 194, at 1913-35.

[224] Id. at 1905.

[225] Bradley, supra note 187, at 297-98(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. F. 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").

[226] Bradley, supra note 187, at 198; Stephen I. Vladeck, The Exceptionalism of Foreign Relations Normalization, 128 Harv. L. Rev. F. 322, 322-23 (2015) (arguing that "foreign relations exceptionalism in contemporary U.S. litigation is alive and well" in the lower federal courts).

[227] Sitaraman & Wuerth, supra note 194, at 1965-66; see also Bradley, supra note 187, 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 previously all-or-nothing nature of the exceptionalism-versus-normalization debate.

* * *

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. Such decisions by private companies will help to determine the extent to which national security creep is presented to the judiciary and the extent to which judges can thus 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. The existence of regulated private parties 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. We return in the conclusion 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.[228] 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.[229] Similarly, less investment ex ante leads to a higher probability of ex post litigation. As others have compellingly

[228] Posner, supra note 26.

[229] Hwang, Unbundled Bargains, supra note 27; Scott & Triantis, Anticipating Litigation in Contract Design, supra note 27; Scott & Triantis, Incomplete Contracts and the Theory of Contract Design, supra note 27; Choi & Triantis, Strategic Vagueness in Contract Design: The Case of Corporate Acquisitions, supra note 27.

argued, in some circumstances, it is rational to skimp on ex ante contract design—for example, if the probability of litigation is very low.[230]

In recent years, scholars have also begun to understand the role that regulators play in contract design and litigation. In previous co-authored work, one of us documented the phenomenon of regulator influence on contract design.[231] 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.[232] 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.[233] 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.[234]

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.[235] And, with very few exceptions, parties bear

---

[230] Id.

[231] Cathy Hwang & Matthew Jennejohn, Contractual Depth, 106 Minn. L. Rev. 1267 (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).

[232] Id.

[233] James Fallows Tierney, Contract Design in the Shadow of Regulation, 98 Neb. L. Rev. __ (forthcoming) (arguing that contracts' audience is sometimes "not courts or consumers, but policymakers deciding whether to reform status quo legal rules from which companies profit").

[234] Jens Frankenreiter, The Missing "California Effect" in Data Privacy Law, __ Yale J. Reg. __ (forthcoming 2022) (finding that despite widespread claims that the European Union's pro-consumer privacy policies would spill over into non-EU jurisdictions, that spillover is significantly less widespread than expected).

[235] One exception is a recent co-authored paper by one of us, which discusses the possibility of public intervention in private contracts in the litigation phase, through contract reformation. 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. See David A. Hoffman & Cathy Hwang, The Social Cost of Contract, 121 Colum. L. Rev. 979 (2020) (noting that the public has several opportunities to intervene in private contracts, including ex ante through laws and regulation, mid-stream through regulatory approval, and, in very rare cases, ex post through contract reformation); see also Cathy Hwang, Comment on The Limits of Public Contract Law, 88 Law & Contemp. Probs. 73 (2022).

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.

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 pre-approval from antitrust authorities—the Federal Trade Commission (FTC) or the Department of Justice (DOJ)—before consummation.[236] 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.[237]

Major transactions—defined by deal size, along with a few other factors—are required to file for pre-approval with antitrust regulators. Filings must be accompanied by a hefty fee that ranges from $45,000 to $280,000, depending on the size of the deal.[238] Once the deal parties make the filing and pay the 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.[239] Otherwise, antitrust authorities might request additional information, ask the parties to make certain modifications to ensure the deal does not have an anticompetitive outcome,[240] or seek to block the deal.[241]

While the pre-clearance process may not always be cheap, easy, or pleasant, its contours are relatively well-understood. Parties with deals of a certain size know to file for pre-clearance and often can predict whether regulators will approve of the deal, or what changes they might request. With

---

[236] Hoffman & Hwang, supra note 235, at 992.

[237] Of course, individual reactions to even the clearest regulation might differ, causing some uncertainty. See Claire Hill, Tax Lawyers are People Too, 26 Va. L. Rev. 1065 (2007).

[238] Fed. Trade Comm'n, Filing Fee Information (March 4, 2021), https://www.ftc.gov/enforcement/premerger-notification-program/filing-fee-information.

[239] Fed. Trade Comm'n, Premerger Notification and the Merger Review Process, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/mergers/premerger-notification-merger-review.

[240] Hoffman & Hwang, supra note 235, at 992-93 (describing the divestments that antitrust authorities required before allowing the 2010 merger of United Airlines and Continental Airlines).

[241] Fed. Trade Comm'n, Premerger Notification and The Merger Review Process, supra note 239.

very few exceptions,[242] 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.

For example, parties are aware that closing certain large deals without antitrust pre-clearance 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.[243] 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 upfront time and money to file for pre-clearance.

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.[244] 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 a private side letter agreement that, until recently, could potentially be kept from regulators.[245] These agreements are another example of ex ante investment that reduces the probability of ex post cost.

---

[242] Buyer Beware: FTC Orders Unwinding of a Consummated Transaction, Cadwalader, Wickersham & Taft LLP (Nov. 7, 2019), https://www.cadwalader.com/resources/clients-friends-memos/buyer-beware-ftc-orders-unwinding-of-a-consummated-transaction (describing eight examples of mergers that have been unwound after consummation between 2012 and 2019).

[243] Fed. Trade Comm'n, The FTC Post Consummation Review Process, https://www.ftc.gov/enforcement/premerger-notification-program/post-consummation-filings-hsr-violations/ftc-post.

[244] Fed. Trade Comm'n, Frequently Asked Questions About Mergers, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/frequently-asked-questions-about-merger-consent-order-provisions.

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

Importantly, parties can engage in this kind of exchange of costs—investing more upfront to reduce ex post cost—because of three important conditions. First, even though most deals are pre-cleared 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.[246] Because parties know where the potential regulatory landmines lie, they can invest upfront to avoid them.[247] Second, antitrust authorities are clear about the types of deals in which they intervene. In fact, they annually publish guidance that clearly sets out which deals need to file for pre-clearance. Finally, for the most part, antitrust regulators predictably intervene one time in a deal—during the ex ante deal design phase. After that intervention, antitrust authorities generally step back, and the parties proceed with their deal without antitrust intervention.[248]

National security review does not enjoy those conditions. For one thing, much of the national security review process is confidential.[249] 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 case challenging CFIUS—*Ralls v. CFIUS*—and its substantive analysis on the government's justification for ordering divestiture is slim.[250] 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.[251] Much of what was not regulated five years ago is now part of CFIUS's purview.[252] Much of what CFIUS has done

---

[246] Fed. Trade Comm'n, *supra* note 239.

[247] Id.

[248] 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; It's a Technical Nightmare, Insiders Say, Wash. Post (Dec. 11, 2020), https://www.washingtonpost.com/technology/2020/12/11/facebook-breakup-antitrust/ (reporting on a rare attempt by the FTC to break up a transaction after it had closed).

[249] U.S. Dept. of the Treasury, supra note 10 (explaining statutorily mandated confidentiality requirements).

[250] Ralls Corp., 758 F.3d at 305; see also supra notes 195-204 (discussing Ralls).

[251] See supra notes 85-86 and accompanying text.

[252] Id.

in the last ten years has been unprecedented, and therefore unexpectable by parties: it 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 Korean-based semiconductor company, Magnachip. 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.[253] Indeed, since 2020, as a result of additional resources from the passage of FIRRMA, CFIUS has doubled its review of so-called non-notified transactions—that is, transactions where the parties did not voluntarily or mandatorily file with CFIUS pre-closing.[254] As one law firm puts it, recent CFIUS activity means that "it is simply getting harder for 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."[255]

Current review processes are also temporally tentacular: CFIUS review can occur at any point during a deal's life, even after closing.[256] And, unlike other countries, where post-closing review can only occur for a few years, CFIUS review can even occur significantly after closing.[257] 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."[258] 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.

---

[253] See infra notes 289-293 and accompanying text.

[254] 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 LLP (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/.

[255] Jalinous et al., supra note 8.

[256] Id.

[257] Cooley LLP, CFIUS Overview, available at https://www.cooley.com/services/practice/export-controls-economic-sanctions/cfius-overview (last accessed Dec. 29, 2021) (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").

[258] Jalinous, et al., supra note 8.

The result of CFIUS's tentacular process is that contract law's well-understood trade-off between ex ante and ex posts costs is upended. When facing a regulatory regime that is as secret, unpredictable, and ever-expanding as CFIUS, parties have a hard time investing upfront 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, it is worth nothing that CFIUS is not the only review process that muddies the trade-off: the U.S.'s 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 both on these and other questions raised by this Essay's account of national security creep.

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,[259] and the "threat" portion of that analysis has been understood to vary based on the country involved in a transaction. 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.[260] 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

[259] See supra notes 56-57 and accompanying text.

[260] Cathleen D. Cimino-Isaacs & James K. Jackson, Cong. Res. Serv., CFIUS: New Foreign Investment Review Regulations 2 (updated May 28, 2020), https://sgp.fas.org/crs/natsec/IF11334.pdf.

Kingdom.[261] 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."[262] That factor clearly references China, and as discussed above, the extant restrictions on outbound investment explicitly target companies linked to China's military.[263]

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. In issuing its investment screening regulation, the E.U. Commission emphasized that while "[n]o specific third country is 'targeted'[,] [c]oncerns relating to security and public order can potentially arise from anywhere."[264] Despite generally strong alliances between the United States and Western Europe, European countries do regard the United States as in some sense a security risk. U.S.-European relations have repeatedly become strained over allegations of U.S. espionage.[265]

Concerns about security threats from the United States may extend to U.S. companies. The U.S. government has in the past solicited and compelled

---

[261] See supra notes 94-100 and accompanying text (discussing excepted foreign states).

[262] John S. McCain National Defense Authorization Act for Fiscal Year 2019, at Sec. 1702(c)(1), Pub. L. No. 115-232, 132 Stat. 1653, 2176.

[263] See supra notes 141-156 and accompanying text.

[264] Communication from the Commission, supra note 105, at 3.

[265] 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 (reporting on allegations, initially published by Der Spiegel, that the United State spied on the EU); 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 (discussing allegations that the United States spied on French government officials and 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); NSA Spying Row: Denmark Accused of Helping US Spy on European Officials, BBC (May 31, 2021), https://www.bbc.com/news/world-europe-57302806; 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/.

assistance from U.S. companies in the service of national security goals.[266] Moreover, the Snowden disclosures also revealed that the National Security Agency "secretly broke[] into the main communications links that connect Yahoo and Google data centers around the world," allowing NSA "to collect at will from hundreds of millions of user accounts,"[267] and that the NSA "inserted a back door into a 2006 [encryption] standard adopted by" the National Institute of Standards and Technology "and later by the International Organization for Standardization."[268]

Given this history, one could imagine that, particularly 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 U.S. government. The very CFIUS-like processes that the United States government has encouraged allies to establish could be turned back against U.S. investors.[269]

A second possible version of blowback comes not from U.S. allies, but from China. As U.S. allies stand up investment reviews with the more-or-less explicit goal of blocking investment from China in particular, the world may move increasingly toward a decoupling of the worldwide economy into economic blocs, a fraught process given the interconnectedness of global

---

[266] 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 Cal. 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" and can resist government demands).

[267] 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.

[268] Nicole Perlroth, Government Announces Steps to Restore Confidence on Encryption Standards, N.Y. Times (Sept. 10, 2013), https://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/?_r=0; see also Larry Greenemeier, NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard, Sci. Am. (Sept. 18, 2013), https://www.scientificamerican.com/article/nsa-nist-encryption-scandal/ (describing how NSA compromised the encryption standard).

[269] Cf. John Kabealo, The Growing Global Alignment in Regulating Chinese Trade and Investment, Atlantic Coun. (June 8, 2021), https://www.atlanticcouncil.org/blogs/the-growing-global-alignment-in-regulating-chinese-trade-and-investment/("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.").

supply chains. China itself restricts foreign investment in certain sectors,[270] but more importantly, one could imagine China pressuring other countries to reject U.S. investment—essentially forcing countries to choose between Chinese investment and U.S. investment.[271] Moreover, adverse decisions on foreign investment may prompt trade-based retaliation, such as restrictions on imports from countries that restrict Chinese investment.[272]

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.[273] 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

---

[270] China updated its Foreign Investment Law in 2019, with changes effective in 2020, and continues to employ a "negative list" system, whereby foreign investment is prohibited or restricted in certain sectors. See generally China: Foreign Investment Law Passed, Library of Cong. (May 30, 2019), https://www.loc.gov/item/global-legal-monitor/2019-05-30/china-foreign-investment-law-passed/ (providing an overview of the Foreign Investment Law); 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; 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).

[271] See, e.g., Kabealo, supra note 269 ("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.").

[272] 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 (reporting Chinese trade restrictions on Australian imports in reaction to, among other things, Australia calling for an investigation into the origins of COVID-19).

[273] 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).

material agreements, which include many M&A agreements.[274] 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 in order 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.[275] 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 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 managing to sometimes evade regulatory scrutiny.[276]

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.[277] 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.[278] 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.[279]

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.[280]

---

[274] 17 C.F.R. §§ 229.10-229.915 (2018) (requiring a disclosure and description of material contracts).

[275] Jeremy McClane, Boilerplate and the Impact of Disclosure on 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").

[276] Hwang & Jennejohn, supra note 231, at 28.

[277] See supra note 243 and accompanying text.

[278] Hwang & Jennejohn, supra note 231, at 26.

[279] Id. at 26-28.

[280] See, e.g., Edmund Lee & Cecilia King, AT&T Closes Acquisition of Time Warner, N.Y. Times (June14, 2018), https://www.nytimes.com/2018/06/14/business/media/att-

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.[281]

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.[282] In the national 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 the 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.[283] However, there is a fair amount of flexibility in disclosure, which means that parties elect to

---

time-warner-injunction.html (reporting on the completion of the AT&T and Time Warner merger, which had previously been blocked by the Department of Justice and was finally allowed after a lengthy litigation).

[281] U.S. Dept. of the Treasury, supra note 10 (explaining statutorily mandated confidentiality requirements).

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

[283] Jeremy McClane, The Sum of Its Parts: The Lawyer-Client Relationship in Initial Public Offerings, 84 Fordham L. Rev. 101, 111 (2015) (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).

disclose less information than they otherwise would, thereby depriving investors of significant marginal disclosures.[284] Furthermore, because there is so much uncertainty about what kinds of transactions will be subject to national security review—and when—there is an incentive for parties 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 national security review process can be obtained—for the right price. As with 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.[285]

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.[286] Securities regulators can create more specific rules about parts of deals that cannot be hidden in side letters.[287] And, finally, investors can work to demand more or better disclosure of deal risks, even though involving national security risk.

---

[284] Id.; 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).

[285] 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 information is, in fact, a way for elite firms to justify their existence. See Elisabeth de Fontenay, Law Firm Selection and the Value of Transactional Lawyering, 41 J. Corp. L. 393, 396 (2015); see also Cathy Hwang, Value Creation by Transactional Associate, 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 (2015).

[286] See supra note 120 and accompanying text.

[287] See supra note 245 and accompanying text.

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.[288]

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.[289] 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.[290] 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.[291] Still, CFIUS asserted jurisdiction and refused to approve the transaction,[292] apparently hinging its jurisdiction on Magnachip's Delaware

---

[288] J. Tyler McGaughey, CFIUS is Preparing to Block China from Acquiring Magnachip Semiconductor Corporation, Winston Strawn LLP (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.

[289] Chase D. Kaniecki, et al., CFIUS Threatens to Block Magnachip Deal; Shows Willingness to Interpret Its Jurisdiction Broadly, Cleary Gottlieb LLP (Sept. 10, 2021), https://www.clearytradewatch.com/2021/09/cfius-threatens-to-block-magnachip-deal-shows-willingness-to-interpret-its-jurisdiction-broadly/; see supra note 253 and accompanying text.

[290] Id.

[291] Id.

[292] See Form 8-K, Magnachip Semiconductor Corp. (Dec. 13, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001325702/000119312521355865/d152828d8k.htm (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"); see U.S. Chipmaker Magnachip, China's Wise Road End $1.4

incorporation, New York Stock Exchange listing, and the fact that the company has a Delaware subsidiary.[293]

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 upfront 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 similar chilling effects might also be diffused alongside the regulatory processes. The more countries 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.

In short, it is hard to tell, at this point, how CFIUS diffusion 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.

IV. 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

---

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/.

[293] 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." Id.; see also 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 (discussing "CFIUS's unprecedented intervention" in the deal).

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 what 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, 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 we address 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 post facto 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 branch officials to be careful with their authorities, they 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 Congress, judges, scholars, and the public. 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 U.S. 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 is 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.

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.