The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections

Samuel J. Rascoff†

For decades, the American intelligence community has adhered to a norm against spying for the sake of enriching private firms. More recently, the norm has figured in a prominent presidential directive as well as in various international agreements. But notwithstanding its durability and its newfound renown, the norm has largely eluded scholarly consideration. In this Essay, I aim to address that gap by showing how theories of agency capture and institutional culture can help make sense of the norm's past and inform judgments about its future.

INTRODUCTION

Traditional separation of powers theory contemplates the allocation of official authority between the constitutionally created arms of government. Recent scholarship extends this discussion to the administrative state.[1] But the concept is rarely employed to consider the relationship between the state and the market.[2] And yet some of the most dynamic and important issues surrounding contemporary national-security law and policy implicate precisely this state-market boundary. In this Essay, I aim to take up the larger themes of the Symposium by illuminating

† Professor of Law, Faculty Director, Center on Law and Security, NYU School of Law. Thanks to the participants in the Symposium and in the Syracuse University workshop on Controlling Economic Cyber Espionage, where I presented an earlier version of this Essay. I am especially grateful to William Banks, Joel Brenner, Rajesh De, Zachary Goldman, Jack Goldsmith, Ryan Goodman, Aziz Huq, Daryl Levinson, Herbert Lin, Jon Michaels, Randal Milch, Jami Miscik, and Stephen Slick for helpful comments and suggestions. Thomas Coyle, Joshua Fattal, David Hoffman, and Jan-Frederik Keustermans provided excellent research assistance.

1 See, for example, Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 Colum L Rev 515, 529–30 (2015).

2 See, for example, Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-First Century* 11–13 (Knopf 2008) (discussing the emergence of the market state); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 Cal L Rev 901, 908–09 (2008) (explaining the relationship between government intelligence agencies and private sector companies).

an aspect of the complex relationship between the market and the national-security state.

My particular focus is on the meaning and functions of a norm that has been around in one way or another for at least forty years but that has recently enjoyed a spate of public attention: the prohibition against collecting intelligence for the sake of enriching American businesses[3] (what I refer to as the "norm"). As former Director of Central Intelligence (DCI) Robert Gates put it: "We do not penetrate foreign companies for the purpose of collecting business information of interest to U.S. corporations. In our view, it is the role of U.S. business to size up foreign competitors' trade secrets, market strategies, and bid proposals."[4]

This self-imposed constraint[5] on the national-security state is, in many respects, peculiar. For one thing, it is curiously gerrymandered to allow certain forms of market-state collaboration but not other forms that are functionally the same. More generally, its stability bucks a decades-long trend in public law and life, in which the barriers between business and government have increasingly subsided.[6]

But the norm is more than a curiosity; it does important work in underwriting—or aspiring to underwrite—our intelligence and cybersecurity strategies.[7] Moreover, American evangelizing on behalf of the norm has apparently paid off: the norm

---

3 See, for example, Randall M. Fort, *Economic Espionage*, in Roger Z. George and Robert D. Kline, eds, *Intelligence and the National Security Strategist: Enduring Issues and Challenges* 237, 237 (Rowman & Littlefield 2006) ("[T]he key issue under consideration is not whether such intelligence should be collected, but rather whether it should be provided by the U.S. Intelligence Community to the private sector."). That said, the norm may constrain collection as well—for example, by curtailing the ways in which the collection priorities of the intelligence community should be influenced by the private sector.

4 *The Threat of Foreign Economic Espionage to U.S. Corporations, Hearings before the Subcommittee on Economic and Commercial Law of the Committee on the Judiciary*, 102d Cong, 2d Sess 53 (1992) ("1992 Economic Espionage Hearings") (statement of DCI Robert M. Gates).

5 Although not a focus of this Essay, the existence of the norm attests to the capacity of constraints to organically emerge from within the intelligence community. See Nathan Alexander Sales, *Self-Restraint and National Security*, 6 J Natl Sec L & Pol 227, 228–29 (2012).

6 See text accompanying notes 68–70.

7 For example, the White House's recently issued Executive Order on cyberhacking sends a clear message to the Chinese government that hacking for private gain is a nonstarter. See generally Executive Order 13694, 80 Fed Reg 18077 (2015). Meanwhile, the US government's "response to penetrations targeting government-held data has been more restrained, in part because U.S. officials regard such breaches as within the traditional parameters of espionage." Ellen Nakashima, *U.S. Decides against Publicly Blaming China for Data Hack* (Wash Post, July 21, 2015), archived at http://perma.cc/9RFT-4HY9.

has recently been adopted by China[8] and the G-20[9] through a series of bilateral[10] and multilateral instruments. In view of its stature at home—and, of late, overseas—the norm warrants careful analysis.

In attempting to explain the norm, former intelligence officials typically advert to its practical importance in avoiding problems of administration. But theoretical accounts—especially in legal scholarship—have been relatively scarce. In this Essay, I take stock of three such accounts. The first, advanced by Professor Jack Goldsmith in a series of recent blog posts,[11] is rooted in international relations realism.[12] The second approach stems from the political science of regulation, and in particular from theories of agency capture.[13] The third is grounded in a cultural-organizational account of American intelligence that emphasizes the reluctance of intelligence professionals to subordinate their efforts to the bottom lines of profit-seeking corporations.[14]

In Part I, I present a brief genealogy of the norm and its evolution before offering an analytic account of the norm as it currently stands (including the considerable exceptions that it admits). In Part II, I advert to some of the more practical explanations that have been summoned on behalf of the norm and then present some potential theoretical justifications. In Part III, I briefly discuss two sets of issues—one strategic, the other institutional—that are currently putting pressure on the norm, even as it enjoys unprecedented publicity.

---

8 See Ellen Nakashima and Steven Mufson, *The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace* (Wash Post, Sept 25, 2015), archived at http://perma.cc/KE7E-J6MV. The agreement particularly bars economic espionage that is "cyber-enabled." Whether China will adhere to the norm in practice remains an open question. See text accompanying notes 86–89.

9 See Ellen Nakashima, *World's Richest Nations Agree Hacking for Commercial Benefit Is Off-Limits* (Wash Post, Nov 16, 2015), archived at http://perma.cc/2F7J-MBG6.

10 In addition to its recent pact with the United States, China has entered into comparable agreements with the United Kingdom and Germany. See Foreign and Commonwealth Office, *UK-China Joint Statement on Building a Global Comprehensive Strategic Partnership for the 21st Century* (Gov.uk, Oct 22, 2015), archived at http://perma.cc/3SNJ-TAM5; John Leyden, *China, Germany Moving Closer to No-Hack Pact* (The Register, Oct 30, 2015), archived at http://perma.cc/9Z37-D34B.

11 See Jack Goldsmith, *The Precise (and Narrow) Limits on U.S. Economic Espionage* (Lawfare, Mar 23, 2015), archived at http://perma.cc/5PN2-QCDA (describing some of the metes and bounds of the norm); Jack Goldsmith, *Reflections on U.S. Economic Espionage, Post-Snowden* (Lawfare, Dec 10, 2013), archived at http://perma.cc/U5HX-JBRA (explicating the realist logic of the norm).

12 See text accompanying notes 64–67.

13 See text accompanying notes 68–70.

14 See text accompanying notes 71–81.

I. A BRIEF GENEALOGY OF THE NORM

The norm against economic espionage for the benefit of private firms first appeared in a public document enjoying the force of law in January 2014, when the White House issued Presidential Policy Directive 28 (PPD-28), its most significant statement of national-security law and policy in the aftermath of the revelations made by Edward Snowden.[15] But the norm dates back at least to the 1970s, a period of intense turmoil and change in the intelligence community. During the Nixon administration, the President's Foreign Intelligence Advisory Board (PFIAB) took up the question of economic espionage in the context of potential responses to the economic threat posed to Detroit by the emergence of Japanese automobile manufacturing.[16] Gerard Burke, who headed the PFIAB, recalled that this body considered the acceptable limits of economic espionage and "discussed it ad nauseam. . . . [The Board] thought U.S. companies needed [support], but [it] didn't think it should be provided by the U.S. government. There were obvious conflicts of interest."[17] As Burke later reported, the PFIAB concluded that US firms would have to forfeit potential economic advantages because it would be inappropriate for the government to share tactical economic intelligence with them.[18] Admiral Stansfield Turner, President Jimmy Carter's DCI, considered abandoning the norm, asking: "[I]f [the economy] isn't a national security matter, then what is!?"[19] But, faced with strong opposition from his senior staff, Turner relented.[20]

---

15 See generally *Directive on Signals Intelligence Activities* (Administration of Barack Obama, Jan 17, 2014) ("PPD-28"), archived at http://perma.cc/8KJP-H2QV. According to PPD-28:

> The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.

Id at *3 (citation omitted).

16 See John J. Fialka, *War by Other Means: Economic Espionage in America* 7 (Norton 1997).

17 Id.

18 *1992 Economic Espionage Hearings*, 102d Cong, 2d Sess at 18 (cited in note 4) (statement of Gerard S. Burke).

19 Fialka, *War by Other Means* at 7 (cited in note 16).

20 Stansfield Turner, *Burn before Reading: Presidents, CIA Directors, and Secret Intelligence* 101 (Hyperion 2005) ("Soon after I suggested doing this, I faced a storm of protests from CIA professionals. They did not see helping business as being part of their mission of promoting national security."). Turner apparently retained this belief even after leaving government. See Amy Borrus, et al, *Should the CIA Start Spying for Corporate*

The issue next came to a head (and generated some public and scholarly attention[21]) in the aftermath of the Cold War, during which "our national security [became] inseparable from our economic security."[22] Under conditions in which certain legislators regarded the CIA as having limited value (at best),[23] a debate emerged about how to deploy the intelligence community in the new strategic environment. As Representative Dan Glickman (who later became Chairman of the House Permanent Select Committee on Intelligence[24]) put it:

> America is much more at risk today by our industrial base being withered away than it is probably by the former Russian empire, and it is important that this country become lean and mean in fighting the economic threats of the rest of the world, particularly when our companies may be the targets of competitors who would think nothing of stealing secrets in a surreptitious way.[25]

In this environment, the administration of President George H.W. Bush released a strategy document that recognized the changing intelligence landscape and openly asked: "What kinds of economic intelligence do we need?"[26] But on the question of the norm, the CIA held firm: former DCI Gates emphasized that "the

---

America?, Bus Week 96, 96 (Oct 14, 1991). Occasionally, a former CIA officer objects to the norm. See, for example, David E. Sanger and Tim Weiner, *Emerging Role for the C.I.A.: Economic Spy* (NY Times, Oct 15, 1995), archived at http://perma.cc/C6WV-Z9UQ (quoting Robert Kohler, a retired CIA official, as asking: "If we're willing to do dirty tricks for the defense part of national security, then why aren't we able to do dirty tricks for the economic part?"). But this perspective is clearly an outlier.

21 See, for example, Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 L & Pol Intl Bus 459, 459–60 (1995) ("[E]conomic espionage has become 'in some ways the hottest current topic in intelligence policy issues.'"); Mark Burton, *Government Spying for Commercial Gain*, 37 Stud Intell 17, 17 (1994) (analyzing the post–Cold War debate over the limits on economic espionage).

22 Warren Christopher, *The Strategic Priorities of American Foreign Policy*, 16 DISAM J 48, 50 (Winter 1993–94).

23 In 1991, Senator Daniel Patrick Moynihan introduced the End of the Cold War Act, which would have, among other things, abolished the CIA. S 236, 102d Cong, 1st Sess, in 137 Cong Rec 1840 (Jan 17, 1991). In 1995, he introduced the Abolition of the Central Intelligence Agency Act. S 126, 104th Cong, 1st Sess (Jan 4, 1995).

24 See *Dan Glickman* (The George Washington University Graduate School of Political Management), archived at http://perma.cc/3RQR-9TMQ.

25 *1992 Economic Espionage Hearings*, 102d Cong, 2d Sess at 5 (cited in note 4) (statement of Rep Glickman, a member of the House Committee on the Judiciary).

26 George H.W. Bush, *National Security Review 29* *2 (The White House, Nov 15, 1991), archived at http://perma.cc/99XT-TLM8.

CIA does not, and will not, engage in commercial espionage."[27] The Clinton administration undertook its own review of the prospects of economic espionage as part of a broader pivot toward emphasizing the role of economic issues in foreign policy.[28] Run by then–National Security Council Senior Director for Intelligence Programs George Tenet, the review focused on "the role that the Intelligence Community should play regarding foreign competitors of American business."[29] In 1993, following the review, DCI Woolsey declared the administration's opposition to "spying on foreign corporations for the benefit of domestic businesses."[30] Two years later, a bipartisan commission reviewing the issue reached the same conclusion. Created by the Intelligence Authorization Act for Fiscal Year 1995,[31] the Commission on the Roles and Capabilities of the United States Intelligence Community reviewed the role of the intelligence community in the "post-cold war global environment"[32] and reported its findings in a report titled *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*.[33] The Commission determined that "the intelligence community's activities in the area of economic intelligence should continue, but that it should have a limited role."[34] The Commission made it clear that "[t]he role of the Intelligence Community is to provide support to the Government, not to the private sector."[35]

Of late, the norm has reemerged in the context of post-Snowden discussions regarding the appropriate metes and bounds of US surveillance and cybersecurity initiatives. Director

---

27 *1992 Economic Espionage Hearings*, 102d Cong, 2d Sess at 53 (cited in note 4) (statement of DCI Robert M. Gates).

28 See R. Jeffrey Smith, *Administration to Consider Giving Spy Data to Business* (Wash Post, Feb 3, 1993), archived at http://perma.cc/A5D8-93VB (noting that then-DCI-designate R. James Woolsey had referred to the issue as "the hottest current topic in intelligence policy" and had pledged that the administration would review the "complexities, legal difficulties [and] foreign policy difficulties" surrounding the norm); Sanger and Weiner, *Emerging Role for the C.I.A.* (cited in note 20).

29 Joseph C. Evans, *U.S. Business Competitiveness and the Intelligence Community*, 7 Intl J Intell & Counterintell 353, 353–54 (1994).

30 Id at 356.

31 Pub L No 103-359, 108 Stat 3423 (1994).

32 Intelligence Authorization Act for Fiscal Year 1995 § 903(a)(1), 108 Stat at 3458.

33 See generally Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (GPO 1996) ("1996 Intelligence Commission").

34 Michael T. Clark, Comment, *Economic Espionage: The Role of the United States Intelligence Community*, 3 J Intl Legal Stud 253, 257 (1997).

35 *1996 Intelligence Commission* at 23 (cited in note 33).

of National Intelligence James Clapper underscored the norm's ongoing relevance to the intelligence community, which was ultimately embodied in PPD-28, the White House's most definitive legal and policy response to the Snowden revelations. As Clapper put it, "[w]hat we do not do . . . is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—US companies to enhance their international competitiveness or increase their bottom line."[36] Prompting this renewed interest in the norm is a sense that political and business audiences at home, and especially overseas, want assurances that the American intelligence community is not employing its formidable electronic surveillance and cybersecurity capacities to give American businesses a leg up in the global marketplace.[37] Furthermore, insofar as the United States is an outlier in adhering to the norm, its prominence in the post-Snowden moment could be seen as an attempt to brand American intelligence as, in some respects, more constrained than counterpart institutions overseas.[38] Whether the target audiences believe the American story is another matter; in the aftermath of the Snowden leaks, the German domestic intelligence service[39] investigated whether the United States was involved in economic espionage against German business.

---

[36] *Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage* (Office of the Director of National Intelligence, Sept 8, 2013), archived at http://perma.cc/NW69-9BNV.

[37] See, for example, Matt Welch, *Switzerland Furious about Snowden's Charge That the CIA Conducts Economic Espionage against Formerly Secret Swiss Banks* (Reason, June 10, 2013), archived at http://perma.cc/J6PF-D4A8; Anthony Boadle, *NSA Spying on Petrobras, If Proven, Is Industrial Espionage: Rousseff* (Reuters, Sept 9, 2013), archived at http://perma.cc/AF6T-B3YF. Conceived of as a source of reassurance to skeptical audiences, the norm can be seen as bearing some conceptual affinity with the recently announced policy that the intelligence community will not employ vaccination programs in operational settings so as not to cast into doubt the integrity of important public health functions. See Lena H. Sun, *CIA: No More Vaccination Campaigns in Spy Operations* (Wash Post, May 19, 2014), archived at http://perma.cc/8BPS-E9RG.

[38] In this connection, it is worth noting that American officials have campaigned on behalf of the norm's global adoption. See *Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues, U.S. Department of State before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*, 114th Cong, 1st Sess *9 (2015) (statement of Christopher M.E. Painter), archived at http://perma.cc/XD7H-NB5L ("A State should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.").

[39] This office is called the Bundesamt für Verfassungsschutz (BfV). Its official website is archived in English at http://perma.cc/539M-E68V and in German at http://perma.cc/M82C-4H5M. The BfV considers economic espionage by foreign states to

It is worth considering a number of aspects pertaining to the status and scope of the norm. First, until the recently issued PPD-28, the norm was never embodied in a statute or executive order.[40] Although intelligence officials frequently describe it in terms that evoke law, the norm is probably best thought of (at least until PPD-28) as reflecting intelligence policy. For that matter, what we know about the norm is largely a product of public statements; compliance is not subject to verification by third parties.[41] Second, the norm is a distinctly American one. As Gates recently explained: "[I]t's hard for people to believe this. You'll have to take my word for it. We are nearly alone in the world in not using our intelligence services for competitive advantage for our businesses."[42] He went on to say that "[t]he Chinese probably have the most pervasive system of collecting against us of any country" but also that "it's important to remember they're not alone."[43] Former head of American counterintelligence Joel Brenner has written that "[t]he Chinese intelligence services are the worst but not the only sponsors of this kind of larceny. The Russian intelligence services are quieter and more selective than the Chinese, but they too are in the business of stealing [intellectual property] for commercial purposes."[44] And as another former CIA director, General Michael Hayden, put it recently, there are only four other countries (presumably the other members of the so-called Five Eyes[45]) that

be a serious threat to the German economy. See *Economic Security* (BfV), archived in English at http://perma.cc/CYF6-EH4Z and in German at http://perma.cc/3G88-MP36.

40 See Goldsmith, *Reflections on U.S. Economic Espionage, Post-Snowden* (cited in note 11) (describing the norm as "a policy without . . . any basis in law").

41 See Zoë Carpenter, *Can Congress Oversee the NSA?* (The Nation, Jan 30, 2014), archived at http://perma.cc/KN3C-GECR (discussing challenges to effective congressional oversight of the intelligence community).

42 Philip Ewing, *Gates: French Cyber Spies Target U.S.* (Politico, May 22, 2014), archived at http://perma.cc/AUH3-SAEE.

43 Id.

44 Joel Brenner, *The New Industrial Espionage* (American Interest, Dec 10, 2014), archived at http://perma.cc/XSM2-VVU9. See also *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* *5 (Office of the National Counterintelligence Executive, Oct 2011), archived at http://perma.cc/78Z2-3349.

45 See Margaret Warner, *An Exclusive Club: The Five Countries That Don't Spy on Each Other* (PBS, Oct 25, 2013), archived at http://perma.cc/NJ4S-GBM5 (describing the "Five Eyes" as a group of five countries—consisting of the United States, the United Kingdom, Canada, Australia, and New Zealand—with a long-standing agreement not to spy on one another).

adhere to a version of the American norm.[46] The secondary literature frequently identifies France as a leading practitioner of economic espionage[47] (something the French do not try to hide[48]), though Israel and Germany are also often mentioned.[49]

Concerning the scope of the norm, a number of (potentially very significant) exceptions characterize this area. The norm focuses on offensive intelligence gathering. In other words, the norm has meant (and apparently continues to mean) that officials are not authorized to seek out intelligence for the benefit of private firms. Nor are company executives permitted to "task" intelligence agencies to acquire secrets on their behalf. Intelligence agents may, however, gather and share information with firms about threats to their businesses. As Gates put it:

> [I]n coordination with the FBI, we inform an individual company if we detect an intelligence operation directed specifically against it overseas. . . . This sometimes requires that the information we provide be in a generic fashion, but we usually find a way to tell the company what it needs to know to take corrective action.[50]

Another carveout pertains to information shared with businesses concerning any alleged involvement of foreign officials in a business matter, including, but not limited to, cases of bribery. As a footnote in PPD-28 explains, "[c]ertain economic purposes, such

---

[46] See *Michael Hayden Says U.S. Is Easy Prey for Hackers* (Wall St J, June 21, 2015), archived at http://perma.cc/5M5Q-TBRH.

[47] See, for example, Hedieh Nasheri, *Economic Espionage and Industrial Spying* 15 (Cambridge 2005) (discussing a 1996 Senate report that described France's "aggressive and massive espionage effort against the United States").

[48] This practice dates back to 1946. See Didier Lucas and Nicolas Moinet, *1994-2014: Quelle organisation de l'intelligence économique d'entreprise en France?*, 70 Géoéconomie 147, 147–48 (2014). For the official statement of the French government, see *Compte-rendu du Conseil des ministres du 29 mai 2013* (Présidence de la République française, May 29, 2013), archived at http://perma.cc/D2RU-Q7UC (stating in relevant part that "engaging in economic intelligence means to collect, analyze, disseminate and protect strategic economic information . . . for the benefit of all economic actors (companies, research institutions, ministries, regions)") (author's translation).

[49] See Anton Troianovski and Harriet Torry, *German Government Is Accused of Spying on European Allies for NSA* (Wall St J, Apr 30, 2015), archived at http://perma.cc/L27K-C2J9 (describing recent accusations that the German intelligence agency helped the NSA monitor "thousands of phone numbers and Internet addresses" related to Germany's European allies); Nasheri, *Economic Espionage and Industrial Spying* at 15 (cited in note 47) (listing Germany and Israel as countries that have been involved in economic espionage against the United States for forty-five years).

[50] *1992 Economic Espionage Hearings*, 102d Cong, 2d Sess at 54 (cited in note 4) (statement of DCI Robert M. Gates).

as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage."[51] In other words, the norm has been and continues to be compatible with robust information sharing in certain cases of perceived economic downsides to businesses (especially noteworthy in an era of pervasive cyberintrusions), but not in connection with providing firms with economic upsides.

Perhaps most significant, the norm is frequently described as preventing American officials from gathering information for the purpose of enriching private firms. As Hayden recently put it, "We only steal stuff to keep you free and to keep you safe. We do not steal stuff to make you rich."[52] But distinguishing sharply between these two goals is not as straightforward as Hayden makes it seem, and as such, the norm admits of potentially very significant exceptions.[53] As a leading intelligence text puts it, "In a market economy, [ ] it is [unclear] which economic issues have national security dimensions that justify or require the involvement of intelligence agencies."[54] For example, the norm appears to be compatible with a strategy that regards the enrichment of certain firms as enhancing national security. As long as the purpose of the intelligence sharing is couched in national-security terms, the fact that a firm or an industry may benefit financially is apparently not problematic.[55]

II. EXPLAINING THE NORM

Why have such a norm? A number of practical accounts have been offered by current and former intelligence officials. Frequently summoned is the explanation that the norm is necessary to avoid the practical puzzle of how to distribute economically beneficial information to American firms in competitive

---

51 *PPD-28* at *3 n 4 (cited in note 15).

52 *Michael Hayden Says U.S. Is Easy Prey for Hackers* (cited in note 46).

53 Deciding when economic affairs count as national-security issues is not unique to this setting. For example, in the context of the Exon-Florio Amendment and the Committee on Foreign Investment in the United States regulations that implement it, "national security" is "interpreted broadly, without limitation to a particular industry." James K. Jackson, *The Exon-Florio National Security Test for Foreign Investment* *3 (Congressional Research Service, Feb 23, 2006), archived at http://perma.cc/5VJS-NN9B.

54 Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence* 6 (Brassey's 3d ed 2002).

55 See Burton, 37 Stud Intell at 18 (cited in note 21) ("[D]efense contractors or other national security-related businesses may be provided government intelligence data because they are required for a special project, such as the development of a weapon system.").

industries.[56] The norm, on this account, is motivated by the desire to prevent the government from facing the dilemma of either creating competitive advantages within industry sectors or sharing intelligence with an entire sector.[57] As DCI Tenet put it in his congressional testimony:

> [I]f we did this, where would we draw the line? Which companies would we help? Corporate giants? The little guy? All of them? I think we quickly would get into a mess and would raise questions of whether we are being unfair to one or more of our own businesses.[58]

But while this practical and (potentially) legal problem of equal treatment captures something true about the complexity of transferring knowledge from the intelligence community to a competitive market, it seems inadequate to justify the emergence and durability of the norm.[59] Not all domestic industries have competitive structures. The very example that national-security officials frequently adduce to explain the norm—namely, that the United States may not spy for the benefit of Boeing vis-à-vis Airbus[60]—is hard to square with this explanation, because Boeing has no significant American competition in its core business.

---

56 See id at 19 ("Any attempt to distribute intelligence would be complex. And issues of fairness would most likely lead to lawsuits and costly court battles in which companies vie for 'national security' status and, thus, intelligence privileges.").

57 A separate practical problem may be defining which global firms are considered American. See Fort, *Economic Espionage* at 241–42 (cited in note 3). But this problem is of a more recent vintage than the norm, and besides, while being complex, it too is hardly insoluble. Public-private relationships in the surveillance and cybersecurity arenas depend on making precisely these sorts of determinations.

58 *DCI Statement on Allegations about SIGINT Activities* (CIA, Apr 12, 2000), archived at http://perma.cc/N7MZ-W9JD.

59 Brenner has argued that the norm tracks conventional understandings of trade law:

> The only economic espionage that offends existing international norms is the stealing of IP for commercial gain—regardless of whether a state or a private actor undertakes it. This is not a self-serving American distinction; TRIPS recognizes the significance of a "commercial purpose" and "unfair commercial use" in establishing violations.

Brenner, *The New Industrial Espionage* (cited in note 44).

60 See David E. Sanger, *Fine Line Seen in U.S. Spying on Companies* (NY Times, May 20, 2014), archived at http://perma.cc/7UQM-8VCH (noting that officials maintain that, under the norm, "while the N.S.A. cannot spy on Airbus and give the results to Boeing, it is free to spy on European or Asian trade negotiators and use the results to help American trade officials—and, by extension, the American industries and workers they are trying to bolster").

A second such explanation emphasizes the need for the norm in order to justify the imposition of American criminal sanctions on foreigners who steal American intellectual property under the Economic Espionage Act of 1996[61] (EEA). As a former State Department employee put it in testimony before the Senate Select Committee on Intelligence, "We cannot engage in behavior that we find reprehensible in others."[62] On this account, penalizing others for misappropriating American know-how would be untenable in a world in which American officials carry out the same sorts of activities. But this account, too, is wanting. First, the EEA is a product of the 1990s, while the norm has been around for decades longer. Second, this demand for the symmetric treatment of foreign and American economic espionage contradicts standard intelligence practice. While it is a crime to spy on the United States,[63] that is obviously no barrier to the work of American intelligence agencies overseas.

When it comes to more-theoretical discussions of the norm's existence and endurance, they have been largely absent (especially in legal scholarship). A notable exception is supplied by Professor Goldsmith, who recently offered an account of the norm that emerges from a tradition of international relations realism:

> On the whole the United States doesn't gain much from stealing trade secrets from foreign firms to give to U.S. firms. But the United States and its firms have a lot to lose when other nations engage in this discrete form of economic espionage against U.S. firms. Thus the best rule for the United States is one that tries to limit this form of economic

---

61 Pub L No 104-294, 110 Stat 3488.

62 Arthur S. Hulnick, *The Uneasy Relationship between Intelligence and Private Industry*, 9 Intl J Intell & Counterintell 17, 19 (1996). A business leader left no doubt as to his desire to criminalize economic espionage: "As we enter the 21st century, the United States must make it a high priority to communicate in no uncertain terms that industrial espionage is unacceptable behavior. The penalties for the practice of economic espionage either by a foreign competitor or U.S. citizen should be stiff and severe." *1992 Economic Espionage Hearings*, 102d Cong, 2d Sess at 123 (cited in note 4) (statement of James E. Riesbeck, Executive Vice President, Corning, Inc). Some commentators have lately called for creative solutions to the asymmetric situation in which the United States adheres to the norm while foreign governments do not. See, for example, Benjamin Wittes, *A Modest Proposal for NSA* (Lawfare, Mar 18, 2014), archived at http://perma.cc/AQA5-F36X.

63 To be certain, foreign spying is not necessarily prosecuted in American courts. But as former Director for Cybersecurity at the National Security Council Robert Knake put it, arrests and expulsions played an important deterrent role in the Cold War. Nakashima, *U.S. Decides against Publicly Blaming China for Data Hack* (cited in note 7).

> espionage. However, economic espionage outside this narrow context—not in order to benefit discrete U.S. firms, but rather to advantage the United States economy and U.S. firms generally on the global scale (in trade negotiations, e.g.)—serves U.S. interests, especially since the [U.S. government] has the most powerful capabilities in this context. And so the [U.S. government] thinks this form of economic espionage is acceptable.[64]

Goldsmith's account is compelling, especially in helping to make sense of aspects of the cyberstandoff between the United States and China.[65] But the realist account has its limitations. For one, it does not adequately explain the norm's staying power over a period of over forty years. As discussed in this Essay, there were key moments in CIA history when the United States would have benefited from relaxing the norm and yet did not, thus confounding realist logic.[66] Second, the realist theory would tend to suggest that economically developed countries adopt the norm as a way of protecting themselves against the theft of intellectual property.[67] But (at least until very recently) America was an outlier in adhering to the norm, and unless this country is unique in having more to lose on balance in a world in which the norm did not exist, realist theory cannot fully account for the norm.

Some other heretofore-unexplored theoretical possibilities present themselves. First is the prospect that the norm can be thought of as an outgrowth of regulatory-capture theory within the intelligence world. Absent the norm, intelligence officials might be vulnerable to capture by the very businesses whose bottom lines American spies would be setting out to improve.[68] The norm, on this explanation, serves to insulate spy agencies from becoming, in effect, extensions of the research and development arms of Boeing, Ford, or IBM. Potentially supporting

---

64 Goldsmith, *The Precise (and Narrow) Limits on U.S. Economic Espionage* (cited in note 11).

65 See, for example, Jonathan Eric Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 Chi Kent J Intel Prop 189, 192 (2009).

66 See text accompanying notes 16–19.

67 A variant on the realist perspective is the idea that the norm enables technological and economic growth, while its absence stifles it. See Burton, 37 Stud Intell at 19 (cited in note 21) ("[I]ntelligence support could actually damage long-term US competitiveness by discouraging innovation and creating a dependence on foreign firms.").

68 See generally Rachel E. Barkow, *Insulating Agencies: Avoiding Capture through Institutional Design*, 89 Tex L Rev 15 (2010). Thanks to Professor Aziz Huq for suggesting this possibility.

such an explanation is a sense that the norm is historically most closely identified with the CIA, as opposed to the largely militarized balance of the intelligence community. It is conceivable that CIA leaders sought refuge in the norm and in its ability to protect their agency from the sorts of dynamics that characterized bureaucratic life in the military-industrial complex. This is not to say that the CIA is, or ever was, cut off from industry.[69] But as compared with other government agencies, including rival intelligence bureaucracies lodged within the military, private interests have arguably exercised less overall influence over the CIA.[70]

Another theoretical account (which potentially complements the capture story) emphasizes the role of institutional culture within the intelligence community in generating and sustaining the norm.[71] The ethos of American spies—especially in the CIA and, more particularly, its operational arm[72]—has traditionally elevated the work of intelligence above the pedestrian affairs of the market (or, for that matter, the balance of the government).[73]

---

69 The CIA backs a venture capital arm that invests in technologies important to the agency and to the intelligence community more broadly. See *About IQT* (In-Q-Tel), archived at http://perma.cc/52FA-ZP8L.

70 See, for example, Turner, *Burn before Reading* at 100 (cited in note 20) (citing, but expressing doubt about, DCI John McCone's claim "that when he was DCI it was CIA policy to refuse all offers of help from corporations and to adamantly tell U.S. corporations to stay out of local politics").

71 Burke, reflecting on the decision of the PFIAB to maintain the norm in the 1970s, mentioned institutional culture as one of the bases for the norm. See *1992 Economic Espionage Hearings*, 102d Cong, 2d Sess at 18 (cited in note 4) (statement of Gerard S. Burke) (describing how the PFIAB had advised the president to maintain the norm, feeling that it was inappropriate for US intelligence agencies to provide information to American companies). For a discussion of the role of institutional culture in shaping national-security policy, see Jeffrey W. Legro, *Cooperation under Fire: Anglo-German Restraint during World War II* 223–29 (Cornell 1995) (identifying areas in which the cultural preferences of the British and German militaries powerfully shaped military and policy choices during World War II); Ryan Goodman and Derek Jinks, *Toward an Institutional Theory of Sovereignty*, 55 Stan L Rev 1749, 1772 (2003) ("Irrespective of its potential strategic value, states no longer recognize assassination as a culturally viable option.").

72 As General Hayden (a career military intelligence officer) put it: "Each of the four big directorates has its own culture." Hayden went on to describe the "'fighter pilot' mystique in the National Clandestine Service" and the "'tenured faculty' mystique in Directorate of Intelligence." Genevieve Lester, *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence* 41 (Cambridge 2015).

73 Similar cultural claims could be made about top-level officials in other agencies, the products of the so-called Establishment. See generally, for example, Kai Bird, *The Chairman: John J. McCloy and the Making of the American Establishment* (Simon & Schuster 1992) (detailing the life of a celebrated member of the Establishment who

Life in the CIA's operational arm entailed unique responsibilities and sacrifices, which officers were prepared to make—but only for the right sort of cause. In the early 1990s, when the end of the Cold War called into question the future of the CIA and when the norm came under intense pressure, former DCI Gates justified the norm in a speech to Detroit business leaders. "Some years ago," he explained, "one of our clandestine service officers overseas said to me: 'You know, I'm prepared to give my life for my country, but not for a company.' That case officer was absolutely right."[74] As another former intelligence officer reasoned, "Intelligence officers sign up to serve their country and defend its security. Can they be convinced that (in some cases) risking their lives—or at the very least their career success—for a company is the same as for their country?"[75]

The self-understanding of CIA officers was that they were members of an elite secret society, handpicked on Ivy League campuses and embodying a spirit of noblesse oblige.[76] As one former member of the CIA's operational arm put it (with particular reference to that branch of the CIA), "The [Directorate of Operations (DO)] is an elite, if narrow, confraternity. . . . [T]here is something *chevaleresque* about being a member of the DO society."[77] In the context of this quasi-religious culture[78] (Hayden, a

undertook numerous senior roles in national security). But at the CIA, this set of habits of mind seems to have shaped the bureaucracy in general, not merely senior leaders.

74 Loch K. Johnson, *The Threat on the Horizon: An Inside Account of America's Search for Security after the Cold War* 103 (Oxford 2011). Furthermore, it may be difficult to persuade others to betray their own countries in the absence of the norm. As a commentator and former intelligence official put it, "Would current and future sources of information want to provide secrets to the U.S. Government if those sources thought the information was only going to advance an American company's bottom line?" Fort, *Economic Espionage* at 243 (cited in note 3).

75 Fort, *Economic Espionage* at 248 (cited in note 3). Former Assistant Secretary of State Randall Fort argues that "economic competitiveness is not a true national security issue, and so is not worthy of application of extraordinary national security measures such as intelligence support." Id at 246. I read his claim—contestable as it obviously is—as much as anything as a manifestation of the ethos on which the norm has historically depended.

76 See Rhodri Jeffreys-Jones, *The CIA and American Democracy* 71 (Yale 3d ed 2003) (noting a concentration of alumni of Harvard, Yale, and Princeton in the elite ranks of the CIA). See also Lester, *When Should State Secrets Stay Secret?* at 44 (cited in note 72) (quoting former CIA official Charles Allen to the effect that CIA officers were "chosen ones").

77 Charles G. Cogan, *The In-Culture of the DO*, in George and Kline, eds, *Intelligence and the National Security Strategist* 209, 213 (cited in note 3).

78 Gates likened the insular "closed circle" of CIA officers to a "priesthood." Joseph E. Persico, *Casey: From the OSS to the CIA* 251–52 (Viking 1990). This trope continues to the present day. See Jo Becker and Scott Shane, *Secret 'Kill List' Proves a Test of*

former CIA director, referred to the agency's work as a "vocation," emphasizing the "religious sense of the word"[79]), the norm makes a lot of sense as a way of ensuring that the sacred work that spies undertake not be somehow profaned by the workings of the market. To spy in order to enrich private firms would be, fundamentally, to misunderstand the value hierarchy of the intelligence cult. The CIA answers to the country's national-security leaders, including the president (and even then, only imperfectly).[80] But it does not answer to the Chamber of Commerce.[81]

It would be too much to claim that the entire historical (or contemporary) record bears out the capture story or the cultural theory of the norm. But some key moments in the norm's history are certainly illuminated by them. For example, it is logical that the norm would have been initially threatened by Admiral Turner, a career military officer who was tapped to head the CIA but was a stranger to its culture.[82] Alarmed at a serious (and politically salient) threat to American economic hegemony—for example, Japanese automobile manufacturing—Turner's attempt to abandon the norm might well have made economic sense. But it was a nonstarter within the CIA, as Turner came to appreciate when his senior staff discouraged him from making this change.[83]

Furthermore, these bureaucratic and cultural accounts help to explain why the post–Cold War CIA declined the invitation extended by a number of congressmen to maintain the agency's ongoing relevance by pivoting aggressively into economic espionage, up to and including carrying out intelligence for the primary benefit of American firms. Such a move would have exposed a

---

Obama's Principles and Will (NY Times, May 29, 2012), archived at http://perma.cc/6YSC-ZLX6 (quoting then–State Department Legal Adviser Harold Koh to the effect that career CIA official and then–counterterrorism czar John Brennan was like "a priest with extremely strong moral values who was suddenly charged with leading a war").

79 Lester, *When Should State Secrets Stay Secret?* at 45 (cited in note 72).

80 See Michael J. Glennon, *National Security and Double Government* 12–13 (Oxford 2015).

81 See Hulnick, 9 Intl J Intell & Counterintell at 27 (cited in note 62) ("Several DCIs have turned to private industry for help in managing the multi-billion dollar intelligence community, and to private academic institutions for review of analysis or for training. But, this has never been a two-way street.").

82 Former Deputy DCI Henry Knoche referred to Turner as belonging to a different "culture." Cogan, *The In-Culture of the DO* at 210 (cited in note 77).

83 See Clark, Comment, 3 J Intl Legal Stud at 264 (cited in note 34). Turner himself remained a believer in economic espionage. As he put it, "We steal secrets for our military preparedness. I don't see why we shouldn't to stay economically competitive." Borrus, et al, *Spying for Corporate America?*, Bus Week at 96 (cited in note 20).

vulnerable CIA to capture by American industry. At the same time, it would have offended the traditional CIA officer's sense of the right ordering of the intelligence domain by threatening to instrumentalize the agency's relationship to the market.

III. CONCLUSION: A NORM ASCENDANT?

In the post-Snowden era, and in recognition of the mounting importance of cybersecurity, the government appears to have doubled down on the norm, especially in its public-facing efforts. And, as noted above, the norm has also exploded on the international scene as of late. But whether the norm ends up redefining intelligence practices overseas, or even proving durable (as a practical matter) at home, may well depend on powerful strategic and institutional factors. Concerning the viability of the norm overseas (and especially in China), it is hard to offer a confident assessment, as a "Cool War"[84]—marked by global competition that coexists with economic interdependence—increasingly defines the relationship between the United States and China. Much may end up turning on the recent agreement between the United States and China on economic espionage.[85] While some officials (notably Director of National Intelligence Clapper[86]) have registered their skepticism that the Chinese are serious about cracking down on economic espionage,[87] certain commentators have expressed cautious optimism that the deal may herald a new era of mutual cooperation.[88] Among the reasons that have been summoned to explain why China might be ready for

---

84 See Noah Feldman, *Cool War: The Future of Global Competition* xi–xiv (Random House 2013) (describing US-China relations as a "cool war" characterized by a struggle for power and a deepening of economic cooperation occurring simultaneously).

85 There is no consensus as to why the Chinese agreed to the deal. For a thoughtful exploration of multiple possible explanations, see Jack Goldsmith, *What Explains the U.S.-China Cyber "Agreement"?* (Lawfare, Sept 26, 2015), archived at http://perma.cc/39XK-JY2E.

86 See Aaron Mehta, *Clapper Skeptical of US-China Cyber Deal* (DefenseNews, Sept 29, 2015), archived at http://perma.cc/PYD5-4XHV. The United States' top counterintelligence officer recently claimed that, in the wake of the deal, "[no]thing has changed." Mark Hosenball, *U.S. Counterintelligence Chief Skeptical China Has Curbed Spying on U.S.* (Reuters, Nov 18, 2015), archived at http://perma.cc/XCY2-A4FD.

87 The language of the pact is sufficiently open-ended as to leave open the possibility that the Chinese will not honor the bargain, at least not in the manner that American officials might expect or hope.

88 See, for example, Stewart Baker, *Steptoe Cyberlaw Podcast, Episode #82: An Interview with Jim Lewis* (Lawfare, Oct 1, 2015), online at http://www.lawfareblog.com/steptoe-cyberlaw-podcast-episode-82-interview-jim-lewis (visited Jan 15, 2016) (Perma archive unavailable).

the norm is the pressure being exerted by that country's rapidly expanding technology industry and by the emergence of greater professionalism among Chinese intelligence agencies.[89] More immediately, China may have reacted to the mounting pressure of American indictments and targeted sanctions.

As to whether the norm can be expected to endure domestically, the answer may depend on what is entailed by the cybersecurity imperative (which is, in part, an artifact of the Cool War). In particular, cybersecurity tends to require ever-greater blurring of the boundaries between public and private actors in the provision of national security.[90] As Hayden put it recently while describing the need for private actors to shoulder responsibility for their own cybersecurity, "The government ain't coming. You're not quite on your own, but you are more on your own [in cyberspace] than you in your lifetime have ever experienced being on your own [as to security in the brick-and-mortar world]."[91] Here is concrete evidence of the emergence of national security under conditions of the "market state," the transition to which "implies a vast increase in the responsibility of private actors, from companies and individuals to [ ] NGOs."[92]

To be certain, the norm, with all of its carveouts and qualifications, is formally compatible with robust cybersecurity. And the imperative to coproduce[93] national security is certainly not new. But the scale of the public-private collaboration in cybersecurity may be unprecedented.[94] The government has made strides to acknowledge this reality. Consider, for example, the recently issued Department of Defense (DOD) cybersecurity

---

89 Notably, in the aftermath of the Chinese hack on the Office of Management and Budget, American officials were quick to point out that (unlike economic espionage for the enrichment of firms) there was nothing awry about the cyberpenetration. As General Hayden put it, "[T]his is not shame on China. This is shame on us for not protecting that kind of information." *Michael Hayden Says U.S. Is Easy Prey for Hackers* (cited in note 46).

90 Cybersecurity has fundamentally altered the nature of the information sought by American businesses from the national-security state. It is no longer the intellectual property of foreign firms that is of central interest so much as it is the information about the threat vectors targeting American businesses for cyberattacks.

91 *Michael Hayden Says U.S. Is Easy Prey for Hackers* (cited in note 46).

92 Gregory F. Treverton, *Intelligence and the "Market State"*, 10 Stud Intell 69, 72 (Winter–Spring 2001). See also Bobbitt, *Terror and Consent* at 85–124 (cited in note 2).

93 For a somewhat different sense of coproduced intelligence, see Samuel J. Rascoff, *The Law of Homegrown (Counter)terrorism*, 88 Tex L Rev 1715, 1720 (2010) (describing the "coproduction" of counterterrorist intelligence that occurs between local populations and local government).

94 See Nasheri, *Economic Espionage and Industrial Spying* at 113, 170–84 (cited in note 47).

strategy document, which clarifies that the private sector has a significant role to play in providing for national security in the cyberarena.[95] And programs across the government, from the FBI[96] to the Department of Homeland Security[97] to the DOD (as well as collaborations between multiple agencies[98]), emphasize the need for effective means of public-private collaboration on cybersecurity issues. Under conditions of pervasive collaboration between the market and the state in the delivery of national security, the norm, which aspires to maintain a separation between those two spheres, may come under increasing pressure.

Changes are also afoot on the institutional level, and these too may carry implications for the norm. On the one hand, there is the phenomenon—closely related to the aforementioned point about the ascendancy of cybersecurity—of the NSA's ever-greater role in the intelligence community. Within the NSA, the norm

---

95 *The Department of Defense Cyber Strategy* *3 (DOD, Apr 2015), archived at http://perma.cc/T7UH-NM3S (describing the DOD's relationship with the private sector as its most important partnership). See also Janet Napolitano, *Demonstrating the Need for the Cybersecurity Legislation* (Department of Homeland Security, Mar 9, 2012), archived at http://perma.cc/U659-C2S9 ("Combating cyber threats is a shared responsibility that requires broad engagement—from government and law enforcement to the private sector and most importantly, members of the public.").

96 See *InfraGard* (InfraGard), archived at http://perma.cc/6L6L-W3GQ:

> InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.
>
> . . .
>
> 350 of our nation's Fortune 500 have a representative in InfraGard.

97 See *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations* *17 (National Infrastructure Advisory Council, Oct 14, 2008), archived at http://perma.cc/C2BR-TB7J:

> The Sector Partnership Model is one of the most comprehensive public-private partnerships undertaken by the federal government, engaging nearly every major sector of the economy and every level of government. It seeks to address the security needs and expectations of a variety of highly diverse businesses, government organizations, and security partners under a common framework.

98 Ellen Nakashima, *Cyber Defense Effort Is Mixed, Study Finds* (Wash Post, Jan 12, 2012), archived at http://perma.cc/N3BU-MRLP ("The Defense Industrial Base cyber pilot includes 17 defense companies, among them Bethesda-based Lockheed Martin, which several years ago had terabytes of data related to the Pentagon's Joint Strike Fighter project stolen from its networks."); *DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities* (DOD, May 11, 2012), archived at http://perma.cc/AU63-XPJK (quoting then–Deputy Secretary of Defense Ashton Carter to the effect that he was "pleased by the deep collaboration between DoD, [the Department of Homeland Security,] and [the Defense Industrial Base] partners" and that "[t]he success of this program encourages us to explore additional ways to enhance the protection of defense industry networks and DoD information").

would not have been terribly meaningful a generation or two ago. That is because the NSA was not extensively gathering foreign corporate secrets until relatively recently, when bulk collection became technologically feasible. Furthermore, unlike the CIA—in which the lives of human assets were on the line and deemed too precious to be sacrificed for espionage in the service of corporate earnings[99]—at the NSA the stakes were typically lower, or at any rate less personal. And as a much larger organization steeped in the cultures of the military and elite mathematics—indeed, one former official referred to it as "probably the biggest employer of introverts"[100]—the NSA hardly exudes Establishment clubbiness or quasi-religious esotericism. Combined with what intelligence scholar Gregory Treverton has referred to as "[t]he National Security Agency's vast capacity to monitor signals"—which he says "is as close as the world has to a capacity to monitor the movements of money across borders"[101]—and in light of the mounting cybersecurity imperative at the NSA, it is likely that the norm will increasingly become fodder for lawyers and legalistic interpretation, rather than a continuing bedrock cultural commitment.[102] Under these specifications, the norm may well fall prey to its generous exceptions.

More generally, the cultural distinctiveness (within the government) of the intelligence community is itself threatened by a larger dynamic of the normalization of the intelligence domain.[103]

---

99 See Sanger and Weiner, *Emerging Role for the C.I.A.* (cited in note 20) ("The agency says it will not ask its officers to risk their lives for companies instead of their country.").

100 Camille Tuutti, *Introverted? Then NSA Wants You* (FCW, Apr 16, 2012), archived at http://perma.cc/V5HA-V5JY (quoting then–NSA Deputy Director Chris Inglis at the Federal Senior Management Conference in Cambridge, Maryland, on April 15, 2012).

101 Bobbitt, *Terror and Consent* at 312 (cited in note 2), quoting Treverton, 10 Stud Intell at 74 (cited in note 92).

102 See Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 Harv Natl Sec J 112, 188–204 (2015) (describing the shortcomings of the NSA's compliance-based culture and examining whether recent reforms will challenge the current cultural restraints).

103 See generally Samuel J. Rascoff, *Domesticating Intelligence*, 83 S Cal L Rev 575 (2010). Cultural change is also afoot within the CIA itself. Commentators have noted that in the post-9/11 period, the CIA's culture has become increasingly defined by its paramilitary function. See Mark Mazzetti, *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth* 4–5 (Penguin 2013). Whether or not this represents a return to the authentic institutional identity that characterized the CIA's predecessor agency (the Office of Strategic Services), it certainly amounts to a profound change in the sensibilities of the Cold War spy agency that privileged espionage and analysis, not targeting and killing. Current CIA Director John Brennan is committed to reversing this trend, and he recently announced significant steps to reorganize the CIA, including in

As I have argued elsewhere,[104] the intelligence community has been characterized as of late by unprecedented levels of transparency and by the emergence of robust interest group politics, with the result that the intelligence domain increasingly resembles the balance of the regulatory state. If I am right that the bureaucratic and cultural distinctiveness of intelligence—and in particular of the CIA—helps to explain the norm's origins and durability, this process of homogenization may undermine it.

the cyberdomain. See Mark Hosenball, *CIA to Make Sweeping Changes, Focus More on Cyber Ops: Agency Chief* (Reuters, Mar 6, 2015), archived at http://perma.cc/V8M7-RC5J.

[104] See Samuel J. Rascoff, *Presidential Intelligence*, 129 Harv L Rev 633, 638–39 (2016).