DOMESTICATING INTELLIGENCE

SAMUEL J. RASCOFF*

ABSTRACT

In the best of circumstances, governing domestic intelligence is challenging. Intelligence sits in an uncomfortable relationship with law's commitment to transparency and accountability. History amply demonstrates that intelligence—including domestic intelligence—frequently begins where the rule of law gives out.

The inherent difficulty of governing intelligence has been unnecessarily exacerbated by a deep-seated and longstanding confusion about what domestic intelligence is. For over a century, policymakers and academic commentators have assumed that it is essentially a form of criminal investigation and that criminal law supplies the logical starting place for its effective governance. Over the years, this faulty premise has fostered a boom-and-bust cycle in intelligence governance; domestic intelligence has been, at different times, effectively out of business or unchecked by law.

This Article introduces a new way to think about domestic intelligence and its governance. Domestic intelligence is a kind of risk assessment, a regulatory activity familiar across the administrative state. Similar to risk assessments in environmental or health and safety law, domestic intelligence seeks to quantify a risk before it materializes, based on the

* Assistant Professor of Law, New York University School of Law. Thanks to participants in faculty workshops and conferences at New York University School of Law, University of California, Berkeley, School of Law (Boalt Hall), and University of Illinois College of Law. Thanks in particular to Rachel Barkow, Simon Chesterman, Dan Farber, Noah Feldman, Barry Friedman, Jacob Gersen, Jack Goldsmith, Moshe Halbertal, Phil Heymann, Stephen Holmes, Sam Issacharoff, Jim Jacobs, Michael Livermore, Roman Martinez, Erin Murphy, Burt Neuborne, Anne O'Connell, Rick Pildes, Richard Posner, Ricky Revesz, Jackie Ross, Stephen Schulhofer, Dick Stewart, Greg Treverton, Rebecca Weiner, Kenji Yoshino, and to numerous former and current intelligence officials who provided comments and stimulated thinking on this subject. Superb research assistance was furnished by Nick Colten, Vesna Cuk, Jason Porta, and Zach Rynar. I am indebted to the editors of the *Southern California Law Review* for their meticulous and insightful work. The Filomen D'Agostino and Max E. Greenberg Research Fund at New York University School of Law provided financial assistance.

careful analysis of aggregative data.

Domestic intelligence as risk assessment in turn necessitates a regulatory approach to intelligence governance. This Article shows how some of the mainstays of administrative law—especially an expansive conception of cost-benefit analysis, judicial review, and pluralism—can and must play a key role in intelligence governance. It contends that intelligence governance must concern itself not merely with producing intelligence that is obtained without illegality or abuse, but also with generating accurate and useful intelligence. This Article makes concrete recommendations for situating these theoretical claims within the institutional landscape of contemporary intelligence practice.

For the foreseeable future, domestic intelligence is here to stay. The need for "domesticating" intelligence is therefore urgent. This Article shows how to do so in a way that reflects an accurate understanding of intelligence and its proper governance.

TABLE OF CONTENTS

I. INTRODUCTION

On December 16, 2005, the *New York Times* published a front-page article describing an intelligence program so sensitive that the newspaper's editors delayed publication for over a year at the request of the White House.[1] The program, which came to be known as the Terrorist Surveillance Program ("TSP"),[2] involved extensive electronic surveillance inside the United States conducted by the National Security Agency ("NSA"). As the article put it, "The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad."[3]

The precise contours of the TSP (and other programs like it, which together formed what has come to be known as the "President's Surveillance Program"[4]) are still largely unknown. What has emerged clearly, however, is that the program operated with almost no oversight. Lawyers, who as a matter of course should have been consulted on the legality of the program, were circumvented.[5] (When concerns about the

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

2. OFFICE OF PUB. AFFAIRS, U.S. DEP'T OF JUSTICE, THE NSA PROGRAM TO DETECT AND PREVENT TERRORIST ATTACKS: MYTH V. REALITY 4 (2006), *available at* http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf (referring to the National Security Agency's activities as the "terrorist surveillance program").

3. Risen & Lichtblau, *supra* note 1.

4. *See* OFFICE OF INSPECTOR GEN., DEP'T OF DEF., ET AL., REPORT NO. 2009-0013-AS, (U) UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 1 (2009), *available at* http://judiciary.house.gov/hearings/pdf/IGTSPReport090710.pdf [hereinafter IG REPORT] (explaining that the President's Surveillance Program included "several different intelligence activities").

5. The initial legal analysis of the program by the Office of Legal Counsel ("OLC") was

program's legality led to more lawyers being informed about the program, more infirmities in its legal basis were discovered, leading to threats of mass resignation and refusals to recertify the program.[6]) The Foreign Intelligence Surveillance Court ("FISC"), which plays a critical role in ensuring compliance with the 1978 law designed to provide a check on domestic electronic spying,[7] was kept out of the loop.[8] Although the "Gang of Eight" congressional intelligence leaders was briefed on the program,[9] the secrecy surrounding it was so intense that the ranking Democrat on the Senate side was reduced to sending a handwritten letter to the vice president expressing his concerns, lest any of his staffers learn of the program's existence.[10]

---

conducted by a single lawyer, Deputy Assistant Attorney General John Yoo. *Id*. at 10. Even Yoo's immediate superior at the OLC, Assistant Attorney General Jay Bybee, was unaware of the existence of the TSP. *Id.* at 10, 14. According to the Inspector General of the Department of Justice ("DOJ"), this arrangement was "extraordinary" and "inappropriate" and led to legal analysis that "at a minimum was factually flawed." *Id*. at 30. Meanwhile, the Acting General Counsel of the NSA and the NSA Inspector General were permitted to know about the program but were denied access to its legal justification. *See* Barton Gellman, *Conflict over Spying Led White House to Brink*, WASH. POST, Sept. 14, 2008, at A1.

6. *See* Daniel Klaidman, *Now We Know What the Battle Was About*, NEWSWEEK, Dec. 22, 2008, at 46 (reporting that beyond the TSP itself, much of the legal concern within the Department of Justice focused on other aspects of the President's Surveillance Program, including an effort to mine vast quantities of electronic communications and records for patterns potentially revealing a threat).

7. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783. The statute has since been substantially overhauled, first on a temporary basis by the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552, then more definitively by the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436. FISA provides for the establishment of the FISC "to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in th[e] Act." FISA § 103(a), 92 Stat. at 1788 (codified at 50 U.S.C. § 1803 (2006)).

8. Although the TSP was not formally presented to the FISC, two successive chief judges of the special court, Lamberth and Kollar-Kotelly, were aware of the TSP's existence and expressed concerns about its legality. Michael Isikoff, *The Fed Who Blew the Whistle*, NEWSWEEK, Dec. 22, 2008, at 40. Eventually James Baker, then head of the DOJ office in charge of processing FISA warrant applications, expressed his concern to Chief Judge Lamberth that TSP-derived information was being used in other FISA warrant applications. Lamberth then warned Attorney General Ashcroft and NSA director Michael Hayden that further use of such information would prompt him to issue an opinion effectively banning the program. *Id.* This threat seemed to temporarily stop the practice of importing TSP information into FISA applications. The practice resumed, however, after Chief Judge Lamberth left the FISC, and was met with criticism by Chief Judge Kollar-Kotelly. *See id.*; Risen & Lichtblau, *supra* note 1.

9. IG REPORT, *supra* note 4, at 23. The "Gang of Eight" refers to the senior members of the Senate and House intelligence committees along with the Senate majority and minority leaders and the speaker of the House and the House minority leader. *See id.* The legal obligation to keep the Gang of Eight informed on covert action was created by the Intelligence Authorization Act for Fiscal Year 1981, Pub. L. No. 96-450, § 501, 94 Stat. 1975, 1981–82 (1980).

10. Charles Babington & Dafna Linzer, *Senator Sounded Alarm in '03*, WASH. POST, Dec. 20, 2005, at A10. Senator Rockefeller's handwritten letter is available at http://www.fas.org/irp/news/2005/12/rock121905.pdf (last visited Mar. 1, 2010). Briefings concerning the TSP seem to have been limited

Not only was oversight tending to ensure the TSP's compliance with law lacking, so too was any meaningful review aimed at determining whether the program was effective and suggesting necessary improvements. Officials intimately involved in the creation of the TSP, such as then–NSA director Michael Hayden, have consistently insisted on the program's utility.[11] But a recently issued report reflecting the judgments of the Inspectors General of multiple intelligence agencies is considerably more equivocal.[12] The report notes that the very secrecy of the program tended to undermine its utility by curtailing the number of analysts who had access to information derived from the program.[13] In the end, proponents of the plan were unable (or unwilling) to point to any specific "counterterrorism successes"[14] brought about by the program.

The experience of the TSP is indicative of a larger problem for national security law and policy: the widening chasm between domestic intelligence practice and domestic intelligence governance.[15] It is no secret that domestic intelligence is back with a vengeance. Whether employing electronic surveillance, human intelligence, data mining, or terrorism "watch-lists," the government has significantly increased its domestic intelligence efforts as part of a broader counterterrorism strategy.[16] In the

---

to the Gang of Eight, *see* IG REPORT, *supra* note 4, at 23, or an even more restricted audience, *see* Babington & Linzer, *supra*. *See also* IG REPORT, *supra* note 4, at 29 (observing that acting Attorney General James Comey thought that parts of the TSP "raised 'serious issues' about congressional notification").

11. *See, e.g.*, Michael Hayden, Op-Ed, *Warrantless Criticism*, N.Y. TIMES, July 27, 2009, at A21.

12. *See* IG REPORT, *supra* note 4, at 33 (stating that the DOJ's Office of the Inspector General "found it difficult to assess or quantify the overall effectiveness of the [TSP] program"); *id.* at 36 (stating that many intelligence community officials "had difficulty citing specific instances where [TSP] reporting had directly contributed to counterterrorism successes").

13. *See id.* at 34.

14. *Id.* at 36. The most that the Inspector General's report offers is that there were several instances in which the TSP *may* have contributed to a counterterrorism success, none of which could be described in the unclassified version of the report. *Id.*

15. Domestic intelligence is not concerned exclusively with terrorism. For example, identifying other countries' spies inside the United States is also a priority. *See* Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, § 101(b)(1)(B), 92 Stat. 1783, 1784 (codified at 50 U.S.C. § 1801(b)(1)(B) (2006)) (defining an "agent of a foreign power" eligible for domestic surveillance to include any person who "acts for or on behalf of a foreign power which engages in clandestine activities in the United States contrary to the interests of the United States"). Post-9/11 discussions, however, as well as this Article, focus on the role of domestic intelligence in counterterrorism. Throughout the Article, I use the word "governance" rather than "oversight" in describing the legal regime under which intelligence operates in order to avoid the too-narrow association between oversight and the prevention of abuse.

16. Besides the TSP, many other domestic intelligence programs initiated after 9/11 have come to public attention. One of the earliest was Total Information Awareness ("TIA"), created by Vice

wake of 9/11, new government agencies with domestic intelligence responsibilities have been created,[17] and others have been substantially retooled to focus on intelligence.[18] State and local governments have also become heavily involved in domestic intelligence activities, either collaboratively with the federal government[19] or independently.[20] The

---

Admiral John Poindexter, director of the Office of Information Awareness within the Department of Defense. John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12. Among other activities, TIA was intended to allow warrantless access by the military to a wide range of government and commercial databases. *See* Philip Shenon with John Schwartz, *JetBlue Target of Inquiries by 2 Agencies*, N.Y. TIMES, Sept. 23, 2003, at C1 (reporting that the Army had asked a defense contractor participating in the development of TIA to hire a subcontractor to mine data from JetBlue Airways). In response to strong public and congressional opposition to TIA, the administration renamed the program "Terrorism Information Awareness." *See* DEF. ADVANCED RESEARCH PROJECTS AGENCY, U.S. DEP'T OF DEF., REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM 1 n.1 (May 20, 2003), *available at* http://w2.eff.org/Privacy/TIA/20030520_tia_report.php. Continued concerns over the scope of the program, and over the resignation of its director after revelations that he planned to set up a futures-trading market for predictions about terrorism and assassination, led to the shuttering of the Defense Department's Office of Information Awareness. *See* Eric Schmitt, *Poindexter Will Be Quitting over Terrorism Betting Plan*, N.Y. TIMES, Aug. 1, 2003, at A11. The data-mining programs may have continued under the TSP. Shane Harris, *TIA Lives On*, NAT'L J., Feb. 23, 2006; Matt Kelley, *Feds Sharpen Secret Tools for Data Mining*, USA TODAY, July 20, 2006, at A5 ("At least five of the data-mining programs [pursued by U.S. intelligence agencies] were developed under a Pentagon program, called Total Information Awareness . . . .").

Additional federal and state post-9/11 domestic intelligence initiatives have included the following: the Operation Terrorism Information and Prevention System ("TIPS"), a plan to "enlist truckers, letter carriers, ship captains and others in reporting suspicious activity to the authorities," Elisabeth Bumiller, *Bush Pushes Volunteerism, but a Senate Seat Shares the Agenda*, N.Y. TIMES, Apr. 9, 2002, at A21; Threat and Local Observation Notice ("TALON") reports, an Air Force program monitoring antiwar groups, *see* Lisa Myers, Douglas Pasternak & Rich Gardella, *Is the Pentagon Spying on Americans?*, NBC NEWS, Dec. 14, 2005, www.msnbc.msn.com/id/10454316; a comparable Army initiative, *see* William Yardley, *Army Looking into Claim That an Employee Monitored U.S. Protest Groups*, N.Y. TIMES, Aug. 2, 2009, at A16 (discussing how information gathered by an Army official regarding individuals who were involved in the peace movement may have been shared with local law enforcement); the Multistate Anti-Terrorism Information Exchange ("MATRIX"), a program to analyze information obtained from state government sources, *see* John Schwartz, *Privacy Fears Erode Support for a Network to Fight Crime*, N.Y. TIMES, Mar. 15, 2004, at C1; and the Department of Homeland Security ("DHS") National Applications Office's domestic counterterrorism satellite surveillance, *see* Audrey Hudson, *Homeland Security Abandons Satellite Surveillance Program*, WASH. TIMES, June 24, 2009, at A3.

17. The DHS and the National Counterterrorism Center are examples.

18. The Federal Bureau of Investigation ("FBI") is an example.

19. *See, e.g.*, Department of Homeland Security, State and Local Fusion Centers, http://www.dhs.gov/files/programs/gc_1156877184684.shtm (last visited Mar. 1, 2010). *See also* Janet Napolitano, Sec'y, DHS, Remarks at the Council on Foreign Relations (July 29, 2009) (transcript available at http://www.dhs.gov/ynews/speeches/sp_1248891649195.shtm) (calling for a "more layered, networked and resilient" response to terrorism).

20. *See, e.g.*, CHRISTOPHER DICKEY, SECURING THE CITY: INSIDE AMERICA'S BEST COUNTERTERRORISM FORCE—THE NYPD 3–4 (2009) (describing the counterterrorism efforts of the New York City Police Department).

resurgence of domestic intelligence has not been accompanied by a corollary growth in intelligence governance, which has created a troubling chasm at the heart of domestic intelligence**.** The vacuum is, in fact, doubly troubling. First, and most obviously, the gap between intelligence practice and governance raises the specter of widespread abuse and diminishment in civil liberties.[21] The history of domestic intelligence in America (and across the world) is replete with instances of the government invoking questionable ends to justify increasingly expansive—and legally troubling—intelligence practices.[22] Indeed, the current vacuum can be seen as the latest development in a historical pattern aptly named the "boom-and-bust cycle" of intelligence governance, where the resurgence of interest in intelligence (motivated by concerns about a particular threat) has typically meant a relaxation of the rules restraining intelligence agencies.[23] This relaxation of limits has, in turn, typically generated periods of abusive practices, followed by inquests and periods of tighter regulation.[24]

The governance vacuum also carries a risk to security: without appropriately scaled and designed governance, intelligence is likely to become nonrigorous and ultimately ineffective at providing policymakers with the informational advantage they need to keep terrorist threats at bay. In other words, the current governance gap in domestic intelligence is a problem not only for people who worry about liberty, but also for those primarily concerned with security.

This Article aims to show the way out of the current vacuum, and even out of the larger historical pattern of boom and bust. Treating as a given that domestic intelligence is here to stay (for the foreseeable future, anyway), it offers a new way to think about domestic intelligence

---

21. *See, e.g.*, LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY 25–29 (2008) (discussing some of the costs of counterterrorism laws in countries such as the United States).

22. As Congressman Rush Holt, member of the House Permanent Select Committee on Intelligence, recently put it, "[T]he intelligence community has not undergone comprehensive examination since [the Church Committee of the mid-1970s] . . . and it needs it." *See* Christopher Hayes, *The Secret Government*, NATION, Sept. 14, 2009, *available at* http://www.thenation.com/doc/20090914/hayes (discussing the evolution of congressional oversight of intelligence gathering agencies since the 1970s).

23. *See* JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 90–98 (2007) (discussing the tension between protecting the country from another attack and staying within the confines of the law).

24. *See, e.g.*, PHILIP B. HEYMANN, TERRORISM, FREEDOM, AND SECURITY: WINNING WITHOUT WAR 138 (2003) (arguing that "a state that relies on intelligence activities instead of criminal investigations is likely to look promising as a more effective way of preventing terrorism, but it would create grave new risks").

governance and domestic intelligence itself.[25] I argue that domestic intelligence is best thought of as a form of risk assessment—a familiar concept from regulatory policy and practice[26]—and that the legal and institutional tools developed within the administrative state are necessary to create an effective and enduring intelligence governance framework. In particular, I contend that an expansive approach to cost-benefit analysis that I refer to as rationality review,[27] judicial review, and public participation made possible by increased transparency ought to play significant roles in reconfiguring the governance of domestic intelligence. Regulatory governance implies more than a set of institutions and practices; it suggests the need to rethink the goal of intelligence governance. Specifically, I claim that domestic intelligence governance should aim to produce intelligence that is obtained in full compliance with the law, but also intelligence that is accurate, efficient, and useful to policymakers. By adopting a regulatory approach to intelligence governance, this Article is instructive in how to avoid the unproductive and constricting debate in which counterterrorism implies either a thorough-going military or criminal approach.[28] Against this backdrop, I argue that

25. My account of intelligence governance is consistent with an emerging discourse that focuses on "intelligence under law." *See, e.g.*, James B. Comey, *Intelligence Under the Law*, 10 GREEN BAG 2D 439 (2007).

26. *See* Matthew D. Adler, *Against "Individual Risk": A Sympathetic Critique of Risk Assessment*, 153 U. PA. L. REV. 1121, 1132 (2005) (referring to risk assessments as "a giant leap forward for public rationality"); Mary Jane Angelo, *Harnessing the Power of Science in Environmental Law: Why We Should, Why We Don't, and How We Can*, 86 TEX. L. REV. 1527, 1546 (2008) ("[R]isk assessment is used in virtually every area of environmental law."). Risk assessment is a contested concept, however, not least because it implicates the complex interplay between science and politics. *See, e.g.*, Jamie A. Grodsky, *Genetics and Environmental Law: Redefining Public Health*, 93 CAL. L. REV. 174, 175–76 (2005) (discussing the application of "toxicogenetics" to risk assessment and explaining that the possibilities presented by science will necessitate making certain policy choices).

27. By "rationality review," I mean to embrace a range of techniques focused on ensuring basic rationality in public processes. Such techniques include, but are not limited to, cost-benefit and cost-effectiveness analyses. I mean to imply no connection between rationality review and rational basis review in constitutional law.

28. Such a debate rages throughout many dimensions of counterterrorism. Specific decisions that turn on this conceptual divide include whether alleged Christmas Day bomber Umar Farouk Abdulmutallab ought to have received a *Miranda* warning, *see, e.g.*, Letter from Eric H. Holder, Jr., Attorney Gen., to Senator Mitch McConnell 1, 3 (Feb. 3, 2010), *available at* http://www.justice.gov/cjs/docs/ag-letter-2-3-10.pdf (explaining that the decision to interrogate and charge Abdulmutallab consistently with federal criminal practice reflected "long-established and publicly known" DOJ policies and arguing that "[n]either advising Abdulmutallab of his *Miranda* rights nor granting him access to counsel prevents us from obtaining intelligence from him"); Letter from Senators Dianne Feinstein and Patrick Leahy to President Barack Obama (Feb. 11, 2010), *available at* http://feinstein.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=08f3b607-a24c-4452-8085-eca761853189; the choice of tribunal (military or civilian) for trying self-confessed 9/11 mastermind Khaled Sheikh Mohammed, *see, e.g.*, Letter from Senators Feinstein and Leahy, *supra*

an overarching regulatory approach that draws on a range of legal tools and methodologies (including those with military or criminal law pedigrees) is a better fit for counterterrorism.[29]

I begin in Part II by describing the vacuum in domestic intelligence governance that has emerged in the last eight years. My claim is that the current vacuum has three main dimensions. First, there is a doctrinal aspect to the vacuum: current law exempts numerous and increasingly relevant categories of intelligence gathering, such as human intelligence and data mining, from meaningful judicial scrutiny. This is at least partly the result of the Supreme Court's ongoing unwillingness to express a view about the status and permissible scope of intelligence under the Constitution. Second, there is an institutional component. Increasingly, important practitioners of contemporary domestic intelligence—including agencies formerly devoted exclusively to foreign intelligence matters, as well as local and state police—function without meaningful oversight. At the same time, organizations that have been called on for a generation to provide governance of intelligence—such as the FISC and the congressional intelligence committees—are not well positioned to shoulder the burden of governing the newly ascendant domestic intelligence apparatus.

Third, and most centrally, the vacuum in intelligence governance has conceptual dimensions. The current patchwork of intelligence governance, which grew up in response to the abuses uncovered in the mid-1970s, continues to focus on the prevention of illegality and the politicization of intelligence. But intelligence governance ought to take broader aim, not just at illegally obtained or badly motivated intelligence, but also at unreliable or inefficient intelligence. In other words, the purpose of intelligence governance should not merely be to ward off bad intelligence; it should also be to promote good intelligence.

More fundamentally still, the current vacuum in intelligence governance is connected to a conceptual problem that has plagued domestic intelligence over the course of its century-old history in the United States:

(encouraging the president to try the plotters of the 9/11 attacks in an ordinary federal criminal proceeding rather than a military tribunal); and whether drone attacks targeting U.S. citizens such as charismatic Imam Anwar al-Awlaki comply with due process, *see, e.g.*, Greg Miller, *U.S. Citizen in CIA's Cross Hairs*, L.A. TIMES, Jan. 31, 2010, *available at* http://www.latimes.com/news/nation-and-world/la-fg-cia-awlaki31-2010jan31,0,6008679.story (noting that al-Awlaki would be among the first Americans targeted for assassination by drone attack).

29. *Cf.* Edward P. Richards, *Public Health Law as Administrative Law: Example Lessons*, 10 J. HEALTH CARE L. & POL'Y 61 (2007) (discussing how public health authorities have relied on administrative law to monitor the progression of diseases and regulate behavior throughout history).

Just what sort of activity is domestic intelligence?[30] At different points in the last century, most notably in the wake of 1970s-era revelations of abusive practices within the intelligence community, American officials and commentators on domestic intelligence imported the tools and conceptual frameworks of criminal law to the universe of domestic intelligence. The intelligence process was assimilated to the investigation of crime, and the modalities of checking state power in this area were largely borrowed from criminal procedure.[31] Neither approach was a very good fit, but they nevertheless endured for a quarter-century of relative stability until they came under increased pressure from the post-9/11 counterterrorism imperative and, specifically, the need to design an intelligence regime equipped to anticipate and help prevent certain high-impact, low-probability events. While as a practical matter the criminal standard has given out, conceptually it continues to dominate thinking about domestic intelligence and its governance.

If the analogy to criminal law has obscured the deep meaning of intelligence and interfered with its proper governance, how should we organize our thinking about domestic intelligence? In Part III, I argue that domestic intelligence is properly regarded as a form of risk assessment, a familiar feature from various regulatory regimes across the administrative state.[32] Domestic intelligence as risk assessment is characterized by three

30. A recent working paper issued by the Council on Foreign Relations notes that "[g]iven the importance of domestic intelligence efforts to the homeland, there is surprisingly little consensus on how to define domestic intelligence." Daniel B. Prieto, Council on Foreign Relations, War About Terror: Civil Liberties and National Security After 9/11, at 45 (Feb. 2009) (unpublished manuscript, *available at* http://www.cfr.org/content/publications/attachments/Civil_Liberties_WorkingPaper.pdf). *See generally* David Heyman, *Finding the Enemy Within: Towards a Framework for Domestic Intelligence*, *in* CTR. FOR STRATEGIC & INT'L STUDIES, 2006 CONFERENCE: THREATS AT OUR THRESHOLD 151 (2006), *available at* http://csis.org/images/stories/HomelandSecurity/071022_Chap4-FindingTheEnemyWithin.pdf (discussing the need to develop a framework to systematize the collection of increasingly important domestic intelligence). More generally, as Central Intelligence Agency ("CIA") veteran Mark Lowenthal has noted, "Virtually every book written on the subject of intelligence begins with a discussion of what 'intelligence' means, or at least how the author intends to use the term. This editorial fact tells us much about the field of intelligence." Kristan J. Wheaton & Michael T. Beerbower, *Towards a New Definition of Intelligence*, 17 STAN. L. & POL'Y REV. 319, 320 (2006) (footnote omitted). *See generally id.* (arguing for the need to have a stable definition of intelligence to reduce uncertainty for decisionmakers).

31. These developments, I contend, are internally connected. The "shape" of domestic intelligence determines the "shape" of domestic intelligence governance, and the means of governing intelligence reify and reinforce specific modalities of practicing domestic intelligence.

32. Domestic intelligence as risk assessment is simultaneously broader and narrower than other conceptions of domestic intelligence. It is broader in that it seeks out all information that may prove beneficial at the level of risk management decisionmaking. It is narrower in that it does not include the interventions that are taken on the strength of the risk assessments. Other scholars appear to include these interventions as part of the domestic intelligence process. *See* GREGORY F. TREVERTON, RAND

main features. First, it is proactive—it seeks to acquire and make sense of information about a hazard before the underlying risk materializes. Second, it is aggregative, meaning that domestic intelligence seeks to acquire vast quantities of data from which to draw informed conclusions. Aggregation is evident in the mass acquisition and computer-driven analysis of telephonic communications, electronic mail, and business records, from which patterns of activity potentially suggesting a terrorist threat can be discerned. The aggregative tendency in intelligence collection and analysis is not, however, limited to electronic communications. It also finds expression in human intelligence, where a newfound focus on identifying social patterns (for example, concerning the "radicalization" of young Muslims) has led officials to collect and analyze intelligence relative to whole communities or neighborhoods in search of meaningful trends (as opposed to intelligence regarding specific individuals about whom officials had already nurtured suspicions).[33] Third, and relatedly, domestic intelligence as risk assessment places a premium on the rigorous analysis of data.

If domestic intelligence is essentially a regulatory activity, it follows that regulatory law should supply the framework for thinking about its proper governance. In Part IV, I set out the basic shape of that framework, drawing on three mainstays of administrative law: rationality review, judicial review of agency action, and public participation underwritten by transparency. Through rationality review, the most important of the three, intelligence governance can address not only issues of economic efficiency and analytic soundness, but also the inevitable tradeoffs implicating basic legal and ethical norms. Because the rationality review I champion is not limited to the patchwork of legal doctrine that has grown up around intelligence, it carries the potential for providing more protection of basic rights than is currently available under the law. For example, rationality review could protect against excessive intelligence gathering through human sources. Additionally, judicial review plays an important role in ensuring that practitioners of domestic intelligence comply, over time, with

---

CORP., REORGANIZING U.S. DOMESTIC INTELLIGENCE: ASSESSING THE OPTIONS 16 (2008). My definition accords with Judge Richard Posner's, who is careful to note that the British Security Service ("MI5") and the Canadian Security Intelligence Service ("CSIS") are properly thought of as security services rather than intelligence agencies because they also undertake certain interventions. RICHARD A. POSNER, COUNTERING TERRORISM: BLURRED FOCUS, HALTING STEPS, at xii (2007).

33. To take a recent example, after a Somali-American teen from Minneapolis carried out a suicide bombing in Somalia, the FBI began monitoring Somali communities across the country. *See* Charlie Savage, *Wider Authority for F.B.I. Agents Stirs Concern*, N.Y. TIMES, Oct. 29, 2009, at A1 ("Instead of collecting information only on people about whom they had a tip or links to the teenager, agents fanned out to scrutinize Somali communities, including in Seattle and Columbus, Ohio.").

their previously approved intelligence mandates.[34] Judicial review of this kind—which resembles, in certain respects, traditional "hard look" review[35]—simultaneously plays to judges' core competencies and addresses one of the key dangers endemic to intelligence activity: the insatiability of intelligence officials' appetite for information. Finally, public participation, made possible by greater transparency, promotes more reliable intelligence (which is less prone to the pathologies of groupthink, for example), while at the same time helping to secure the legitimacy of the necessarily secretive intelligence apparatus.

Regulatory governance of domestic intelligence may strike some as farfetched; in fact, however, there have been subtle but important intimations of a regulatory turn in intelligence governance in recent years. In Part V, I note some of these changes by way of offering an account of what regulatory governance of domestic intelligence would look like in practice. The rationality review that I endorse should be performed by an organization within the Office of the Director of National Intelligence ("ODNI"), modeled on the Office of Information and Regulatory Policy ("OIRA") within the Office of Management and Budget ("OMB"). Like OIRA, the office I envision would be tasked with considering costs and benefits (measured in terms of monetary costs as well as more qualitative effects on security and basic rights) of proposed domestic intelligence programs and approving only those programs whose benefits outweigh their costs. Although such an office does not currently exist, the ODNI's organic statute clearly countenances the sorts of analysis that it would perform. Indeed, the ODNI's *raison d'être* is to lead the intelligence community's efforts in budgeting, intelligence sharing, analysis, and the protection of civil liberties—precisely the sorts of issues central to effective rationality review of intelligence programs. I argue that by taking on responsibility for rationality review of domestic intelligence programs, the ODNI will be able to answer an open question concerning the office's proper role in relation to the intelligence community. Next, I contend that the FISC ought to provide the sort of judicial review of agency action that I advocate, building on important transformations in that court's role brought about by the FISA Amendments Act of 2008. Finally, and somewhat more

34. In an important sense, judicial review is a special case—albeit the most significant one—of a larger phenomenon: compliance-based review. *See* James A. Baker, *Symposium Introduction: Intelligence Oversight*, 45 HARV. J. ON LEGIS. 199, 202 (2008) (oversight is centrally "about knowing whether [intelligence agencies] have complied with the [relevant] rules").

35. *See* Motor Vehicle Mfrs. Ass'n of the U.S. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 42–44 (1983) (stating that "reasoned analysis" requires that agencies must thoroughly consider relevant facts and alternatives).

tentatively, I offer a thumbnail sketch of what a more transparent and pluralistic intelligence governance framework might look like in practice.

I conclude in Part VI by locating regulatory intelligence governance within the larger context of a societal debate that has been raging since 9/11 about the nature of counterterrorism. Is counterterrorism a form of law enforcement *in extremis*? Or (as the previous administration advocated) is it essentially a military enterprise? I contend that neither view gets it right. Instead, counterterrorism ought to be seen as a form of risk management that inevitably draws on a wide range of interventions (including, but certainly not limited to, the tools of war and criminal law enforcement) in order to minimize the threat of attack. Domestic intelligence as risk assessment provides the analytical tools to support the risk-centric approach to counterterrorism that I defend.

Recent scholarship on domestic intelligence has been concerned mainly with issues of institutional design.[36] Specifically, commentators have focused on whether the Federal Bureau of Investigation ("FBI") ought to continue to function as the lead domestic intelligence agency, even as it retains responsibility for federal law enforcement.[37] Questions of

36. *See* POSNER, *supra* note 32 (making structural suggestions regarding the reorganization of intelligence); RICHARD A. POSNER, REMAKING DOMESTIC INTELLIGENCE (2005) (arguing for the creation of a domestic intelligence agency); TREVERTON, *supra* note 32 (laying out the considerations for creating a domestic intelligence agency separate from law enforcement). *See also* MARKLE FOUND., PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (2002), *available at* http://www.markle.org/downloadable_assets/nstf_full.pdf (proposing a networked, decentralized system of information collection, analysis, and sharing); WILLIAM E. ODOM, FIXING INTELLIGENCE: FOR A MORE SECURE AMERICA (2003); James Burch, *A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security*, HOMELAND SECURITY AFF., June 2007, art. 1, http://www.hsaj.org/pages/volume3/issue2/pdfs/3.2.2.pdf; Siobhan Gorman, *FBI, CIA Remain Worlds Apart*, NAT'L J., Aug. 2, 2003, *available at* http://www.govexec.com/dailyfed/0803/080103nj1.htm (noting how the differences between the organizational cultures of the FBI and CIA impair the effectiveness of intelligence and proposing solutions). The debate about institutional design continues to carry practical implications. Siobhan Gorman, *Obama Picks Military Man, Blair, as Top Spymaster*, WALL ST. J., Dec. 20, 2008, at A4 (reporting that "the Obama team is weighing whether to propose the creation of a domestic intelligence agency"). For an important recent article on the redesign of intelligence oversight mechanisms, see Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655 (2006) (discussing the complex interplay between the newly reorganized intelligence bureaucracy and its congressional overseers).

37. *See* ALFRED CUMMING & TODD MASSE, CONG. RESEARCH SERV., REPORT NO. RL33033, INTELLIGENCE REFORM IMPLEMENTATION AT THE FEDERAL BUREAU OF INVESTIGATION: ISSUES AND OPTIONS FOR CONGRESS 15 (2005), *available at* http://www.fas.org/sgp/crs/intel/RL33033.pdf (identifying "synergists," who advocate a combined intelligence–law enforcement mission, and "skeptics," who oppose it); STEPHEN J. SCHULHOFER, THE ENEMY WITHIN 67 (2002). *See also* Harvey Rishikof, *The Role of the Federal Bureau of Investigation in National Security*, *in* INTELLIGENCE AND NATIONAL SECURITY STRATEGIST: ENDURING ISSUES AND CHALLENGES 125 (Roger Z. George &

institutional design are of enormous importance, no doubt, and in certain respects coalesce with the more conceptual approach that this Article adopts. But addressing the conceptual issues indirectly (if at all) as a function of their institutional corollaries has tended to obfuscate the central points that this Article aims to make. While an emerging literature focuses on the way in which counterterrorism participates in a risk-regulatory economy,[38] very little attention has been paid to the way in which intelligence functions as a form of risk assessment or to how the risk-assessment model can inform the way that domestic intelligence is and ought to be governed and legitimized.[39]

More generally, much of the commentary on domestic intelligence has tended to focus on one or another aspect of intelligence tradecraft—especially electronic eavesdropping[40]—to the exclusion of more comprehensive analyses of domestic intelligence as such. By suggesting a new regulatory model of domestic intelligence and domestic intelligence governance, this Article adopts a more holistic approach to the subject, taking aim at the conceptual heart of a problem that has plagued lawyers, policymakers, and citizens for over a century.

II. THE GOVERNANCE VACUUM IN DOMESTIC INTELLIGENCE

Recent years have witnessed the emergence of a governance vacuum in domestic intelligence, underwritten by a phenomenal expansion in intelligence practice, and accompanied by sporadic growth and occasional backtracking in intelligence governance. The expansion of intelligence practice since 2001 was, in a sense, inevitable, in view of the widespread judgment (including by the 9/11 Commission itself) that the 9/11 attacks

Robert D. Kline eds., 2006).

38. *See* Eric A. Posner, *Fear and the Regulatory Model of Counterterrorism*, 25 HARV. J.L. & PUB. POL'Y 681, 696 (2002) (arguing that the regulatory agency mode in which "a special government agency or existing agencies . . . enact regulations to reduce the risk of terrorist attacks or the resulting harm" would be more effective than the current legal model); Jessica Stern & Jonathan B. Wiener, *Precaution Against Terrorism*, 9 J. RISK RES. 393, 441 (2006) (calling for a "systematic analysis of [the] benefits, costs and risks before [making important counterterrorism decisions]").

39. A notable exception is THE CHALLENGE OF DOMESTIC INTELLIGENCE IN A FREE SOCIETY: A MULTIDISCIPLINARY LOOK AT THE CREATION OF A U.S. DOMESTIC COUNTERTERRORISM INTELLIGENCE AGENCY (Brian A. Jackson ed., 2009).

40. Academic focus on electronic surveillance rather than human intelligence probably reflects the way in which the former is considerably more regulated than the latter. This distinction does not necessarily obtain overseas. *See, e.g.*, Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493 (2007) (presenting an empirical comparison of the practice and treatment of undercover policing in the United States and Germany).

were made possible by a series of intelligence failures.[41] The stagnation of intelligence governance has been just as pronounced. To a large degree, the recent renaissance of domestic intelligence was achieved precisely by sloughing off elements of the prior governance regime designed specifically to curtail domestic intelligence. The ascendance of a domestic intelligence apparatus untethered from the governance regime intended to rein it in has revealed—in fact, has helped to create—a troubling vacuum at the heart of domestic intelligence governance. Doctrinal, institutional, and conceptual factors have all contributed to the emergence of this state of affairs.

A. THE DOCTRINAL VACUUM

The first sense in which a governance vacuum has emerged is doctrinal. Simply stated, the current law of domestic intelligence is unable to provide the underpinnings of a meaningful regime to govern collection and analysis of that intelligence. Three distinct aspects of this doctrinal vacuum—each connected to a line of Supreme Court precedents—bear mentioning.

1. Silence from the Supreme Court

Fundamentally, the doctrinal vacuum in intelligence governance derives from the Supreme Court's unwillingness to define the constitutional status of intelligence. In *Katz v. United States*, the Supreme Court embraced the idea that the Fourth Amendment applies to electronic surveillance.[42] The *Katz* Court explicitly declined to weigh in on whether the holding applied to cases "involving the national security."[43] Five years later in the *Keith* case, the Supreme Court expressed the view that the Fourth Amendment does apply in cases "deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the

41. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 76–80, 86–93 (2004), *available at* http://www.911commissio.gov/report/911Report.pdf [hereinafter 9/11 COMMISSION REPORT].

42. Katz v. United States, 389 U.S. 347 (1967).

43. *Id.* at 358 n.23. When Congress acted the following year to pass Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197, 211–25 (codified at 18 U.S.C. §§ 2510–2520 (1968)), it also explicitly disclaimed any position on the role of the Fourth Amendment in electronic surveillance designed for intelligence gathering. *See id.* § 2511(3) (amended 1978) ("Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, [or] to obtain foreign intelligence information deemed essential to the security of the United States . . . .").

existing structure of government."[44] But in so holding, the Court once again clarified that it was expressing "no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."[45] As a practical matter, Congress partially plugged this gap in 1978 when it passed the Foreign Intelligence Surveillance Act ("FISA"), which mandated a procedure for intelligence gathering that resembled a Fourth Amendment warrant procedure in instances where the government sought to obtain "foreign intelligence information."[46] But the legislative solution could not resolve the underlying constitutional puzzle. Indeed, it was precisely this gap in the heart of constitutional doctrine vis-à-vis intelligence that Bush administration officials exploited in arguing for the legality of the TSP.[47] The fact that the Supreme Court has never clarified (and, in fact, has consistently avoided clarifying) the precise legal status of intelligence continues to be an obstacle for meaningful intelligence governance.[48] More recently, the FISA

---

44. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 309 (1972) (quoting the affidavit provided to the Court by the U.S. Attorney General). The Court recognized, however, the ways in which criminal investigation and intelligence diverge, including that

> the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. . . . [Thus,] Congress may wish to consider protective standards for [domestic security surveillance] which differ from those already prescribed for specified crimes in Title III.

Id. at 322.

45. *Id*. at 308. Although this Article is about domestic intelligence in the sense of intelligence learned domestically and pertaining to the prevention of acts of terror on American soil, much of the intelligence I discuss would technically qualify as foreign intelligence under *Keith*. More generally, commentators and intelligence professionals have questioned the utility of the domestic/foreign intelligence distinction in light of the emergence of international terrorism as a leading national security threat. *See, e.g.*, 9/11 COMMISSION REPORT, *supra* note 41, at 400–01 (calling for "unifying strategic intelligence and operational planning . . . across the foreign-domestic divide"). Tellingly, President Obama recently merged the White House Homeland Security Council, which was created during the previous administration and which focused exclusively on domestic issues, with the National Security Council. *See* Helene Cooper, *In Security Shuffle, White House Merges Staffs*, N.Y. TIMES, May 27, 2009, at A13 (noting the statement of President Obama's national security advisor that "terror around the world doesn't recognize borders").

46. 50 U.S.C. § 1804(a)(6)(A) (2006).

47. *See, e.g.*, U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf (arguing that the TSP was consistent with prevailing constitutional and statutory law).

48. In addition to the uncertain status of intelligence in American constitutional law, the status of domestic intelligence under international law is itself hardly clear. Nothing on the order of the strong international norms that pervade other parts of the counterterrorism apparatus—such as the norms against harsh interrogation and detention without due process—can be found in the area of domestic intelligence or of intelligence more broadly. For an interesting attempt to generate an international law of intelligence, see generally Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071 (2006) (discussing the status of

Court of Review has held that the Fourth Amendment warrant requirement is not triggered when the government collects national security–related intelligence "reasonably believed to be located outside the United States."[49]

2. Human Intelligence

While the Supreme Court has never weighed in on the constitutional status of intelligence as such, the passage of FISA did at least usher in a complex regulatory framework for the governance of surveillance of electronic communications such as telephone calls and emails. Yet, as to the conduct of human intelligence—the use of government informants and secret agents to collect intelligence on individuals and groups—the statute is silent, and there is no other statute that speaks to the regulation of intelligence obtained by human sources. Not only has the Supreme Court not afforded protections against government snooping through undercover agents or confidential informants; it has also explicitly exempted human intelligence, or "humint," from coverage by the First and Fourth Amendments.[50] While the FBI has historically imposed limits on its own ability to conduct human intelligence gathering by requiring criminal predication before a source could be injected into a group, for example, those internal rules have been substantially relaxed in the years following 9/11.[51] This gap in doctrine is especially striking in view of the mounting importance of human intelligence as part of a broader counterterrorism strategy.[52] Because of the complex ideational factors surrounding the production—and, therefore, the detection and prevention—of contemporary terrorism, human intelligence, with its ability to shed light on the nuances of human behavior and motivation, supplies potentially critical

intelligence under international law).

49. *In re* Directives to Section 105B of the Foreign Intelligence Surveillance Act, 551 F. 3d 1004, 1012 (FISA Ct. Rev. 2008).

50. Laird v. Tatum, 408 U.S. 1 (1972) (holding that alleged victims of improper government surveillance could not succeed in bringing a claim that the intelligence gathering chilled speech in contravention of the First Amendment); United States v. White, 401 U.S. 745, 752 (1971) (holding that testimony heard by a government agent monitoring a radio transmitter carried by an undercover government informant was not barred by the Fourth Amendment given that "[i]nescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police"); Hoffa v. United States, 385 U.S. 293 (1966) (finding no Fourth Amendment violation where incriminating testimony was heard by an undercover government informant in a hotel room).

51. *See infra* Part II.C.1 (discussing the ATTORNEY GENERAL'S GUIDELINES).

52. For a provocative attempt to work around this doctrinal gap, see David A. Harris, *Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11*, 34 N.Y.U. REV. L. & SOC. CHANGE (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1330023 (calling for negotiated agreements between intelligence and local communities concerning the use of informants).

information.

3. Third-Party Records and Data Mining

The third significant gap in intelligence law relates to the Supreme Court's exemption of third-party records from Fourth Amendment protections. In *Smith v. Maryland*, the Supreme Court held that a pen register is not a search under the Fourth Amendment because there is no legitimate expectation of privacy when information is turned over to a third party, such as a telecommunications firm.[53] Regardless of the practical implications of the exception at the time *Smith* was decided, the widespread availability of enormous volumes of data from third-party providers—and the emergence of technologies to analyze that data wholesale—has opened a significant gap in intelligence governance in recent years. Academic proposals abound to bring data mining within the ambit of the Fourth[54] (or possibly even the First[55]) Amendment. Others recommend a statutory fix to the problem.[56] In the meantime, data mining of third-party records exposes another serious doctrinal limitation in contemporary intelligence governance: there is no current law regulating the extent to which or the manner in which the government can permissibly analyze data legally obtained from third parties.

B. THE INSTITUTIONAL VACUUM

A second dimension of the vacuum in intelligence governance pertains to institutions—both those institutions that perform intelligence functions and those that participate in intelligence governance. The imperviousness of some of the former to governance, and the inability of some of the latter to provide it, has exacerbated the governance vacuum in recent years.

1. Ungoverned Institutions

Lacking a dedicated domestic intelligence agency on par with the

53. Smith v. Maryland, 442 U.S. 735 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301(a), 100 Stat. 1848, 1868–72.

54. *See, e.g.*, Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008) (suggesting ways in which Fourth Amendment doctrine might be read to regulate data mining).

55. *See, e.g.*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008) (arguing for the use of First Amendment norms to protect against certain kinds of network analysis).

56. *See, e.g.*, NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 44–66 (2008) [hereinafter PROTECTING INDIVIDUAL PRIVACY] (proposing a framework to govern the use of data-mining and information-based programs to combat terrorism).

Security Service in the United Kingdom ("MI5") or the Canadian Security Intelligence Service ("CSIS"), American domestic intelligence is performed by a wide variety of organizations with a range of jurisdictions and mandates. Some of this bureaucratic complexity owes to post-9/11 developments at the national level. First, this period has witnessed the creation of new intelligence agencies, such as the Office of Intelligence and Analysis within the Department of Homeland Security ("DHS"),[57] the National Counterterrorism Center within the ODNI,[58] and the National Security Branch within the FBI.[59] Second, federal agencies nominally devoted exclusively to overseas intelligence gathering have been brought into the business of domestic intelligence.[60] Both of these trends have placed additional stress on an already fragile governance structure.

Developments at the subnational level have also contributed to the increased institutional complexity of domestic intelligence. Whether through their own dedicated intelligence arms or through collaborations with the federal government,[61] nonfederal actors have reasserted themselves in American domestic intelligence after a generation-long hiatus.[62] Many of the local agencies that play a role in domestic intelligence have no formal governance regime whatsoever. Others, such as

57. *See* Department of Homeland Security, Office of Intelligence and Analysis, http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm (last visited Mar. 1, 2010) (explaining the role of the DHS and the Office of Intelligence and Analysis in intelligence gathering and analysis).

58. *See* National Counterterrorism Center, About Us, Strategic Intent, http://www.nctc.gov/about_us/strategic_intent.html (last visited Mar. 1, 2010) (describing how the Center works to combat terrorism and share information with other U.S. agencies that are working to prevent terrorist attacks both at home and abroad).

59. *See* Federal Bureau of Investigation, National Security Branch, http://www.fbi.gov/hq/nsb/nsb.htm (last visited Aug. 17, 2009) (discussing the National Security Service ("NSS") and how it works to combine intelligence gathering and terrorist screening under one senior FBI official who reports to the president).

60. *See supra* notes 1–14 and accompanying text (discussing the TSP).

61. Some examples of such collaboration are the DHS's Fusion Centers, the FBI-led Joint Terrorism Task Forces, and the Interagency Threat Assessment and Coordination Group. *See* Information Sharing Environment, Interagency Threat Assessment and Coordination Group, http://www.ise.gov/pages/partner-itacg.html (last visited Mar. 1, 2010). For a critique of how DHS Fusion Centers have operated, see *What's Wrong with Fusion Centers*, ACLU, Dec. 5, 2007, http://www.aclu.org/privacy/gen/32966pub20071205.html.

62. The participation by state and local agencies in intelligence functions is hardly new. Antiradical "red squads" were, at different points in the twentieth century, standard features of major metropolitan police departments. *See* RICHARD E. MORGAN, DOMESTIC INTELLIGENCE: MONITORING DISSENT IN AMERICA 83–85 (1980) (quoting the common term for local police units that monitored dissent). In the wake of revelations of abusive practices, many of these intelligence programs were effectively shut down in the 1970s and 1980s. *See generally* Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 CORNELL L. REV. 735 (1984) (discussing the legal response to the use of surveillance tactics in Chicago, Memphis, and New York during the 1970s).

the intelligence arms of certain large metropolitan police departments, are governed by consent decrees entered into a generation ago in order to resolve civil rights lawsuits. These consent decrees arguably never provided meaningful day-to-day governance, in part because enforcement depended on the vigilance of resource-constrained private plaintiffs. Furthermore, in recent years some of these decrees (including the consent decree binding the New York Police Department's ("NYPD's") Intelligence Division) have been substantially rolled back,[63] further calling into question their utility as tools of intelligence governance. Combined with the absence of agencies at the state and local level that are well positioned to understand and cabin the discretion of intelligence officials, local and state police represent an effectively ungoverned arm of the domestic intelligence apparatus.[64]

2. Ungoverning Institutions

If one aspect of the institutional vacuum is due to the growing number of agencies practicing domestic intelligence that resist governance, the other concerns the limitations of organizations nominally performing the governance function. While a range of executive agencies and officials have historically played a role in the governance of domestic intelligence,[65] for a generation the two most prominent institutional actors have been the federal courts—specifically the FISC—and the House and Senate Select Committees on Intelligence.[66] Although the courts and Congress continue

63. *See* Handschu v. Special Servs. Div., 605 F. Supp. 1384 (S.D.N.Y. 1985) (approving a settlement delimiting police authority to conduct certain kinds of surveillance), *aff'd*, 787 F.2d 828 (2d Cir. 1986), *modified*, 273 F. Supp. 2d 327 (S.D.N.Y. 2003) (granting wider discretion to police following the 9/11 attacks). In 2002, seventeen years after the *Handschu* decree governing the NYPD's Intelligence Division was entered, the NYPD successfully petitioned the court to relax aspects of the decree. *See Handschu*, 273 F. Supp. 2d 327. For a general history of the *Handschu* litigation and consent decree, see Jerrold L. Steigman, Note, *Reversing Reform: The* Handschu *Settlement in Post–September 11 New York City*, 11 J.L. & POL'Y 745 (2003). The consent decree governing the Chicago Police Department's intelligence work followed a similar trajectory. *See generally* Alliance to End Repression v. City of Chi., 237 F.3d 799 (7th Cir. 2001) (Posner, J.) (explaining the need to revisit the strictures of the original consent decree). *See also* Adrian Vermeule, Commentary, *Posner on Security and Liberty:* Alliance to End Repression v. City of Chicago, 120 HARV. L. REV. 1251 (2007) (discussing the impact of Judge Posner's decision on intelligence gathering).

64. A particularly egregious example of ungoverned subnational intelligence work is supplied by the Maryland State Police, who maintained a database in which groups such as bicycle lane advocates and death penalty opponents were labeled terrorists. *See* Lisa Rein & Josh White, *More Groups Than Thought Monitored in Police Spying*, WASH. POST, Jan. 4, 2009, at A1 (discussing the widespread monitoring of advocacy groups engaged in by the Maryland State Police).

65. These include the Inspectors General of the FBI and DOJ, the Attorney General, and the president's Foreign Intelligence Advisory Board.

66. The prominence of the courts and Congress in intelligence governance in some ways depends

to have important roles to play as part of an overall system of intelligence governance, both have serious limitations in their ability to lead the effort. If anything, these limitations have become more pronounced in recent years.

Ever since it was created by FISA, the main purpose of the FISC, which is comprised of eleven Article III judges,[67] has been to consider applications for electronic surveillance of specific individuals (or even more narrowly, their specific telephones or computers) alleged to be "agents of a foreign power,"[68] a statutory term of art which also includes international terrorists, including those who lack formal ties to established terror organizations.[69] Once the FISC approves an application—which it has historically done with respect to over 99 percent of the applications brought before it[70]—its governance role is effectively over. In other words, the FISC provides an ex ante check on the intelligence apparatus without any meaningful follow-up review.[71] The FISC having authorized a particular application, intelligence officials are essentially on their own to determine what they will and will not do.[72]

---

on the logic of separation of powers, a key feature of American governance.

67. 50 U.S.C. § 1803(a) (2006).

68. *Id.* § 1804(a).

69. *See id.* § 1801(b)(1)(C). Dubbed the "lone wolf" provision, this part of FISA was added by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, sec. 6001, § 101(b)(1), 118 Stat. 3638, 3742. *See generally* ELIZABETH B. BAZAN, CONG. RESEARCH SERV., REPORT NO. RS22011, INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: "LONE WOLF" AMENDMENT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2004), *available at* http://www.fas.org/irp/crs/RS22011.pdf (discussing the addition of a new definition of "agent of a foreign power" under FISA).

70. For example, in 2007 the FISC entertained over 2300 applications and denied only three. *See* Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney Gen., to Richard B. Cheney, President, U.S. Senate 1 (Apr. 30, 2008), *available at* http://epic.org/privacy/terrorism/2007fisa-ltr.pdf. That said, the rate at which FISA applications are approved is comparable to federal approval rates for search warrants more generally. *See* 2008 ADMIN. OFFICE OF U.S. COURTS WIRETAP REP. 32 tbl.7, *available at* http://www.uscourts.gov/wiretap08/contents.html. It appears that the Canadian equivalent of the FISC is just as generous in approving warrant applications as the FISC. *See* PETER GILL, POLICING POLITICS: SECURITY INTELLIGENCE AND THE LIBERAL DEMOCRATIC STATE 170 (1994). Former Attorney General Mukasey rejected the suggestion that the government's nearly flawless record in front of the FISC implies that the DOJ is too timid in approaching the FISC with applications where the presence of probable cause is less than clear. *See* Letter from Michael B. Mukasey, Attorney Gen., to Raymond W. Kelly, NYPD Comm'r 1–2 (Oct. 31, 2008), *available at* http://online.wsj.com/public/resources/documents/WSJ_200811202Kelly.pdf.

71. *See, e.g.*, Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 963–65 (2008) (calling attention to the benefits that would be derived from adding additional ex ante review by the FISC). As discussed below, telecommunications firms in receipt of directives from the FISC may challenge those directives.

72. As discussed below in Part IV, this narrow focus on ex ante approvals of intelligence warrants was revisited in the 2008 amendments to the FISA statute.

If the FISC is limited by its focus on the front end of the intelligence process, the other federal courts have a different set of institutional limitations when it comes to governing intelligence. The sort of governance they are qualified to provide, namely entertaining civil suits alleging that specific intelligence programs exceed legal limits, faces three interconnected hurdles. First, and most basically, individuals who allegedly are being spied on illegally tend to be unaware of that fact.[73] Second, if certain individuals have some basis for thinking that they have been the subjects of illegal surveillance, they are often unable to make the kind of definitive showing of injury to satisfy the test for constitutional standing.[74] Third, even if they can meet the test, the government is free to invoke the state secrets privilege and, in effect, unilaterally have the case dismissed on the ground that its resolution by the court might expose necessarily secret information.[75] Taken together, these hurdles make the federal courts inadequate overseers of intelligence. Therefore, neither ex ante review of the sort provided by the FISC nor the exceedingly narrow ex post review provided by ordinary federal courts is sufficient to provide a robust institutional basis for intelligence governance.

The congressional intelligence committees came into being as part of the intelligence governance reforms of the late 1970s.[76] These committees

---

73. It is no accident that the Supreme Court's most significant pronouncements on terrorism issues in the aftermath of 9/11 have all involved challenges to detention. *See, e.g.*, Boumediene v. Bush, 553 U.S. 723 (2008); Hamdi v. Rumsfeld, 542 U.S. 507 (2004). Unlike individuals who fear they are improperly under government surveillance but typically lack definitive proof that that is so, individuals alleging that they are being detained in violation of law know that they are being detained.

74. This hurdle prevented the plaintiffs from being able to litigate the merits of their claims in *ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007). With regard to the plaintiffs' breach of privacy claim under the Fourth Amendment, the Sixth Circuit in *ACLU* held that the plaintiffs lacked standing because they could not make a showing of individual, particularized injury. *Id.* at 673. *See generally* Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992) (discussing the constitutional requirements of standing).

75. *See, e.g.*, *ACLU*, 493 F.3d at 653 ("[T]he plaintiffs do not—and because of the State Secrets Doctrine cannot—produce any evidence that any of their own communications have ever been intercepted by the NSA, under the TSP, or without warrants."). *See also id.* at 650 n.2 (explaining the two applications of the state secrets privilege). The state secrets doctrine originated in *United States v. Reynolds*, 345 U.S. 1 (1953), in which the Supreme Court held that the U.S. government could block the admission or disclosure of evidence that it asserts must remain a national security secret.

76. The Senate Select Committee on Intelligence ("SSCI"), a direct outgrowth of the celebrated Church Committee, came into being in 1976. The House Permanent Select Committee on Intelligence ("HPSCI") was inaugurated the following year. *See* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at 20 (1976), *available at* http://aarclibrary.org/publib/contents/church/contents_church_reports_book2.htm [hereinafter CHURCH COMMITTEE REPORT] (stating that "[c]lear legal standards and effective oversight and controls are necessary to ensure that domestic intelligence activity does not itself undermine the

were intended as a check against flagrant abuse of the sort that came to light during the Church Committee hearings.[77] But from the very start, the intelligence committees faced a number of structural obstacles. First, membership on the committees was term limited.[78] As the *9/11 Commission Report* observed, many intelligence committee members "believe[d] [term] limits prevent [them] from developing the necessary expertise to conduct effective oversight."[79] Second, the purview of the committees was limited to the oversight of very specific aspects of intelligence practice, such as covert action undertaken by the Central Intelligence Agency ("CIA").[80] Third, to the extent that the committees also functioned as watchdogs on the lookout for abuse, the investigative powers they wielded would typically not be used until after alleged abusive practices were publicly revealed.[81] As recent events amply demonstrate, committee members (regardless of party) are poorly incentivized to question intelligence practices that come close to the line of legality, if they

democratic system it is intended to protect"); *id.* at 294 (reiterating the Committee's position "that the Senate create a permanent intelligence oversight committee"); *id.* at 339 ("The Committee reendorses the concept of vigorous Senate oversight to review the conduct of domestic security activities through a new permanent intelligence oversight committee.").

77. The committees were created after the Church Committee was charged with considering "whether intelligence activities threaten the 'rights of American citizens.'" *Id.* at 1 (quoting the Senate resolution creating the Church Committee). For an exhaustive history of the relationship between the CIA and Congress, see L. BRITT SNIDER, CIA, THE AGENCY AND THE HILL: CIA'S RELATIONSHIP WITH CONGRESS, 1946–2004 (2008) (discussing the evolution of the CIA's relationship with Congress from the creation of the CIA to 2004).

78. A standard term of membership on the SSCI was eight years. JUDY SCHNEIDER, CONG. RESEARCH SERV., REPORT NO. RS21908, SENATE SELECT COMMITTEE ON INTELLIGENCE: TERM LIMITS AND ASSIGNMENT LIMITATIONS 3 (2004), *available at* http://www.au.af.mil/au/awc/awcgate/crs/rs21908.pdf. In the House, no member may serve on the HPSCI for more than four out of six consecutive Congresses, except for the chairman and ranking minority member, who have no term limits. H.R. RULE X(11)(A)(4) (2009), *available at* http://www.rules.house.gov/ruleprec/111th.pdf; JUDY SCHNEIDER, CONG. RESEARCH SERV., REPORT NO. RS22123, HOUSE SELECT COMMITTEE ON INTELLIGENCE: LEADERSHIP AND ASSIGNMENT LIMITATIONS 2 (2005), *available at* http://www.fas.org/sgp/crs/intel/RS22123.pdf. In 2004, the Senate revisited the structure of its intelligence committee, making a number of changes including the abolition of term limits. *See* S. Res. 445, 108th Cong. (2004) (enacted); O'Connell, *supra* note 36, at 1713–14. The current iteration of the rules can be seen at S. DOC. NO. 111-3, at 159 (2009). There is no reference to term limits.

79. 9/11 COMMISSION REPORT, *supra* note 41, at 103.

80. *See id.* ("The House and Senate select committees on intelligence . . . have limited authorities.").

81. Oversight of this sort—relying on what Mathew McCubbins refers to as "fire alarms"—typically depends on a public that is positioned to observe official actors and to call attention to their potential abuses. *See generally* Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 166 (1984) (setting out two distinct varieties of oversight). Neither condition is met in the case of the sort of secret activities and information that are the stock and trade of intelligence. More generally, owing to the classified nature of much of intelligence, whistle blowing may involve a violation of a criminal statute.

do not cross it.[82] Fourth, intelligence committees lack the budgeting authority that can provide oversight with teeth. Fifth, the committees lack robust staffing, putting them at a disadvantage in attempting to govern a vast and unwieldy intelligence arm, and what staff is on hand is frequently denied access to the most classified briefings.[83] In addition to the evident limitations of these specialized committees, there is the larger problem that domestic intelligence oversight is furnished by a wide range of committees and subcommittees—a congressional mirror image of the fragmentation that exists within the intelligence community itself. According to a recent study, no fewer than seventeen committees have oversight responsibilities for intelligence matters.[84] Although substantive overlap may have certain benefits, it tends to sap the vitality of the oversight function by diffusing responsibility.

C. THE CONCEPTUAL VACUUM

Finally, and most significantly, the current vacuum in domestic intelligence governance is the product of two deep-seated conceptual gaps—one having to do with the nature of domestic intelligence governance, the other concerning the nature of domestic intelligence itself. The conceptual confusion with respect to the nature of intelligence governance refers to the tendency to think of its purpose in narrow terms: as being solely concerned with forestalling or preventing abuse rather than also aiming to improve the quality and efficiency of intelligence. The confusion with respect to the nature of domestic intelligence refers to the tendency to see domestic intelligence as a species of criminal investigation. Though these conceptual problems are analytically distinct, both, in fact, have historical origins in the so-called criminal standard in domestic intelligence—the (mistaken) idea that criminal law supplies a sound model for thinking about domestic intelligence and its governance.

---

82. *See, e.g.*, Carl Hulse, *Pelosi Says She Knew of Waterboarding by Early 2003*, N.Y. TIMES, May 15, 2009, at A20 (noting that intelligence committee members were briefed early on concerning the use of waterboarding); Douglas Jehl, *Among Those Told of Program, Few Objected*, N.Y. TIMES, Dec. 23, 2005, at A21 (noting the lack of protest on the part of intelligence committee members about the TSP).

83. As former counterterrorism official Richard Clarke has explained, "Essentially what happens, you're a member of the Gang of Eight. You get a phone call: 'We have to come and brief you.' They ask you to go to the vault. They brief you. You can't take notes, you can't have your staff there and you can't tell anybody." Hayes, *supra* note 22 (reporting Richard Clarke's discussion of the shortcomings of the current congressional oversight of intelligence gathering).

84. *See* O'Connell, *supra* note 36, at 1662. Thus, DHS intelligence is subject to oversight by Homeland Security Committees, the FBI by the Judiciary Committees, and military intelligence by the Armed Services Committees.

1. The Criminal Standard and "Oppositional" Intelligence Governance

On December 1, 2008, new *Attorney General's Guidelines for Domestic FBI Operations* came into effect, representing a direct challenge to the criminal law model of intelligence governance.[85] The most notable change the guidelines ushered in[86] was the authorization of FBI agents to engage in proactive intelligence gathering in a manner "not limited to 'investigation' in a narrow sense," with an eye to "provid[ing] critical information needed for broader analytic and intelligence purposes."[87] As one former FBI official put it, thanks to the 2008 guidelines, "The FBI has been entrusted with unparalleled authority to 'chase the threat' without the constraints that governed the agency for many years."[88]

Understanding why these constraints ever came to be necessary implicates path dependency.[89] At different historical moments over the

85. *See* ATTORNEY GEN.'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 8 (Dep't of Justice 2008), *available at* http://www.usdoj.gov/ag/readingroom/guidelines.pdf [hereinafter ATTORNEY GEN.'S GUIDELINES] (explaining that FBI "investigations . . . often serve important purposes outside the ambit of normal criminal investigation and prosecution, by providing the basis for, and informing decisions concerning, other measures needed to protect the national security").

86. For the first time, a single set of guidelines covers all aspects of the FBI's investigative work, including criminal investigations, organized crime matters, and domestic intelligence gathering. *Id.* at 6; Dep't of Justice, Fact Sheet: Attorney General Consolidated Guidelines for FBI Domestic Operations (Oct. 3, 2008), *available at* http://www.justice.gov/opa/pr/2008/October/08-ag-889.html. Beginning with the first guidelines issued in the 1970s by Attorney General Edward Levi, there had always been separate procedures covering discrete areas of Bureau activity. ABRAM N. SHULSKY & GARY J. SCHMITT, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE 149 (3d ed. 2002).

87. ATTORNEY GEN.'S GUIDELINES, *supra* note 85, at 16. This process of relaxing the criminal standard in the guidelines began during the Reagan years and took on more urgency after the Oklahoma City bombing, when FBI director Louis Freeh concluded that the existing guidelines "would allow the FBI to begin an investigation of a group advocating violence to achieve social or political objectives somewhere short of an imminent violation of federal law, if it was apparent the group had the ability to carry out its objectives." *See* SHULSKY & SCHMITT, *supra* note 86, at 156. After 9/11, Attorney General John Ashcroft made further changes. *See* John Ashcroft, Attorney Gen., Remarks on the Attorney General Guidelines (May 30, 2002) (transcript available at http://www.fas.org/irp/news/2002/05/ag053002.html) (stating that after 9/11 "we understood that the mission of American justice and law enforcement had changed" and noting that many FBI agents had expressed "frustrat[ion]" that "internal restrictions," including the investigative guidelines, "hampered our ability to fight terrorism"). Nevertheless, the criminal standard in domestic human intelligence gathering endured to a greater or lesser degree until Attorney General Michael Mukasey definitively renounced it in the most recent version of the guidelines. *See supra* note 85 and accompanying text.

88. Michael Rolince, *New FBI Powers: A Necessary Step for Counterterrorism*, WASH. INST. FOR NEAR EAST POL'Y, Oct. 28, 2008, http://www.washingtoninstitute.org/templateC05.php?CID=2951.

89. *See, e.g.*, Simone Ghezzi & Enzo Mingione, *Embeddedness, Path Dependency and Social Institutions: An Economic Sociology Approach*, 55 CURRENT SOC. 11, 18–19 (2007) (discussing path dependency as a "historically selective process within which some embedded conditions are transformed into specific institutional configurations of development" and "[a]daptation continues to

better part of a century, opponents of domestic intelligence saw the imposition of the criminal standard as a means of neutralizing the tendency of domestic intelligence to threaten civil liberties.[90] Three historical moments are especially salient. The first dates back to the origins of the FBI in the early twentieth century. In response to alleged intelligence abuses by the FBI during the "Red Scare," then–Attorney General Harlan Fiske Stone implemented a form of the criminal standard in 1924, mandating that the FBI not be concerned with the opinions of individuals, political or otherwise, but "only with their conduct and then only with such conduct as is forbidden by the laws of the United States."[91] Gathering intelligence without an allegation of criminal activity would create an agency that was, to Stone, "dangerous to the proper administration of justice and to human liberty, which it should be our first concern to cherish."[92]

This so-called Stone Line did not last long, however. In the second salient moment—which was, in many respects, a reaction to the first—a young, ambitious lawyer at the FBI named J. Edgar Hoover, who began his career in the FBI's intelligence service, was appointed FBI director in 1924[93] and rejected the limitation of intelligence collection to criminal

---

modify the various starting conditions through paths where choices and opportunities are given neither by individual utility nor by predetermined social institutions").

90. By the "criminal standard," I mean the position that authority to engage in intelligence gathering is necessarily tied to an allegation of criminal wrongdoing. To speak of the rise (and fall) of the criminal standard is not to suggest, of course, that criminal law itself has been static or that many of the ideas that I associate with the regulatory paradigm are not also characteristic features of contemporary criminal law. *See, e.g.*, Lousie Amoore & Marieke de Goede, *Governance, Risk, and Dataveillance in the War on Terror*, 43 CRIME L. & SOC. CHANGE 149, 149–50 (2005) (observing that the emergence of risk assessment in counterterrorism is, from the perspective of criminologists, "nothing new"); Paul H. Robinson, Commentary, *Punishing Dangerousness: Cloaking Preventive Detention as Criminal Justice*, 114 HARV. L. REV. 1429, 1429–32 (2001) (arguing that criminal justice is increasingly characterized by a preventive, as opposed to a punitive, mission). Indeed, there is irony in that even as domestic intelligence was increasingly defined by a criminal standard, criminal law itself was in the process of evolving in the direction of a regulatory model. In England, for example, as the "fire brigade" approach to policing proved inadequate in the 1980s,

> fresh emphasis was given to aspects of policing which more closely resemble the security intelligence process . . . [including] the use of stop and search, detention for purposes of interrogation, and attempts to develop local intelligence systems . . . . The other main managerial innovation of the 1980s was "policing by objectives" which is based on research, the analysis of information, the establishment of policy objectives, and the collection and evaluation of information relating to the achievement or otherwise of those objectives.

GILL, *supra* note 70, at 211 (footnote omitted).

91. JOHN T. ELLIFF, THE REFORM OF FBI INTELLIGENCE OPERATIONS 31 (1979).

92. *Id*.

93. *See id.* at 16; MORGAN, *supra* note 62, at 27. The General Intelligence Division was formally created by Attorney General A. Mitchell Palmer in 1919, a quarter-century before the CIA came into being. *See* MORGAN, *supra* note 63, at 27.

investigation that the Stone Line mandated.[94] By the mid-1930s, when FDR was determined to have the FBI collect the intelligence necessary to understand the threat posed by communists and fascists,[95] the criminal standard had been effectively abandoned. Thus, in 1941, Hoover was reminding Attorney General Robert Jackson of the difference between investigation and intelligence gathering, noting the importance of the latter to address the problem of subversive groups that "direct their attention to the dissemination of propaganda . . . much of which is not a violation of a Federal Statute."[96]

The third decisive moment came during the 1970s, following the "fires of controversy created by Watergate, COINTELPRO, and the fifty-year litany of abuses meticulously documented in the Church Committee Report,"[97] when two new governance regimes were ushered in, both tending to instantiate the criminal standard. First, there was FISA, which, as previously discussed, relied on a process similar to that employed under Title III for obtaining criminal wiretapping authority, thereby reinforcing the ways in which the criminal law shaped the governance of intelligence.[98]

---

94. For example, in 1936, Hoover instructed field offices to utilize all possible sources of information pertaining to the subversive activities of leftist and fascist groups advocating the overthrow of the U.S. government. *See, e.g.*, WILLIAM W. KELLER, THE LIBERALS AND J. EDGAR HOOVER: RISE AND FALL OF A DOMESTIC INTELLIGENCE STATE 58–59 & nn.101–02 (1989).

95. *See id.* (stating that FDR reportedly requested "a broad picture of the [communist and fascist] movement and its activities as may affect the economic and political life of the country as a whole").

96. Memorandum from J. Edgar Hoover, Dir., FBI, to Robert Jackson (Apr. 1, 1941), *as quoted in* ATHAN THEOHARIS, THE QUEST FOR ABSOLUTE SECURITY 53 (2007).

97. *See* Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 486 (2006). As the Church Committee explained:

> COINTELPRO is the FBI acronym for a series of covert action programs directed against domestic groups. In these programs, the Bureau went beyond the collection of intelligence to secret action defined to "disrupt" and "neutralize" target groups and individuals. The techniques were adopted wholesale from wartime counterintelligence, and ranged from the trivial (mailing reprints of *Reader's Digest* articles to college administrators) to the degrading (sending anonymous poison-pen letters intended to break up marriages) and the dangerous (encouraging gang warfare and falsely labeling members of a violent group as policy informers).

SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, FINAL REPORT: SUPPLEMENTARY DETAILED STAFF REPORTS OF INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 3 (1976), *available at* http://aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_0_Title.pdf.

98. The emergence of the criminal standard in FISA—its heavy reliance on the modalities of criminal procedure to govern domestic intelligence gathering—helps to explain the emergence of the so-called FISA wall, by which the FBI's criminal investigations were cordoned off from its intelligence gathering. *See* Piette & Radack, *supra* note 97 (discussing the circumstances of the rise of the well-documented "wall" between intelligence and law enforcement). It was precisely because the intelligence methodology was so similar to the criminal methodology that it seemed perverse to be able to take advantage of the lower thresholds for obtaining specific information through one regime as

Second, and less well known, was the promulgation of internal FBI guidelines requiring a showing of criminal predication before human intelligence gathering could commence.[99] Attorney General Edward Levi issued the "Domestic Security Guidelines,"[100] which required that domestic intelligence gathering take place only where criminal predication existed.[101] Geoffrey Stone explains that "[t]he Levi Guidelines embodied values similar to those affirmed by Attorney General Harlan Fiske Stone in 1924."[102] While some argued that the Levi Guidelines did not go far enough to reinstate the criminal standard and protect civil liberties,[103] the

---

against the other. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 916 (4th Cir. 1980) (affirming a district court decision that the FBI had to obtain a warrant when its "primary purpose" shifted from foreign intelligence to criminal investigation); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 488 (2006) (noting that intelligence and law enforcement "merge in th[e] area [of investigation]" (footnote omitted) (quoting S. REP. NO. 95-701, at 9 (1978))).

99. Although the standard historiography tells that the changes in intelligence practice and culture resulted from rules passed in the wake of the major inquests of the mid- to late-1970s, certain studies by other scholars suggest a different possibility. To these scholars, criminal regulation did not precipitate the change in intelligence methodology but rather followed on the heels of using domestic intelligence as a tool for gathering criminal-type information, especially as to the Ku Klux Klan in the wake of the church bombings. According to John Elliff, some within the FBI felt that

> the Klan's activities were essentially a law enforcement problem, and that the transfer [of resources from the Intelligence Division to address the problem of the Klan] would dilute the Intelligence Division's major responsibility for dealing with foreign threats. Those who opposed the transfer lost and they traced many of the division's subsequent difficulties to this "substantial enlargement" of its responsibilities.

ELLIFF, *supra* note 91, at 79–80 (footnote omitted). Either way, the period witnessed what a leading scholar has called the FBI's transformation from a "bureau of internal security," with its connotation of a technocratic office, into a political police and what he dubs "a state within a state." KELLER, *supra* note 94, at 154. *See also* THEOHARIS, *supra* note 96, at 221 ("In the immediate aftermath of the Church and Pike committee exposés, Congress appeared ready to enact a charter law.").

100. *See* ELLIFF, *supra* note 91, at 29–30, 60. According to Elliff, Levi's commitment to restoration of the criminal standard and to disavowing the intelligence function of the FBI was such that he did not want the guidelines to be referred to as the "Domestic Intelligence Guidelines." *See id.*

101. *See* SHULSKY & SCHMITT, *supra* note 86, at 151 ("The key point in the Levi Guidelines is that investigation of such groups is permitted only when a group (or an individual) is or may be engaged in activities 'which involve or will involve the use of force or violence and which involve or will involve the violation of federal law.' This is the essence of the criminal standard that effectively defines the government's interest in the domestic security area." (quoting the Levi Guidelines)). Specifically, the Levi Guidelines authorized the FBI to collect "information on the activities of individuals, or the activities of groups, which involve or will involve the use of force or violence and which involve or will involve the violation of federal law." ELLIFF, *supra* note 91, at 61.

102. GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 555 (2004) (criticizing the tendency to exaggerate foreign threats in order to build up support for executive action). It is noteworthy, perhaps, that Levi and Harlan Fiske Stone were both academic lawyers (and law school deans) naturally suspicious of intelligence operations not tethered to alleged criminal law violations.

103. For example, Elliff (himself a staff member on the Church Committee) expressed the view that

> [i]t is not enough to say that the FBI shall investigate only where it has credible information or reasonable suspicion that a crime has been or may be committed. Nor is it adequate to say

changes evidently brought about a fundamental reorientation of domestic intelligence away from "strategic intelligence" and toward case-specific information. The reestablishment of the criminal standard meant that the FBI essentially got out of the business of gathering and analyzing broad-gauged strategic information against potential threats and assimilated its intelligence gathering to the methodology of criminal investigation. As an FBI official recently observed, in determining the presence and magnitude of a terrorism threat in a specific part of the country, the relevant criterion under the criminal standard was the number of terrorism-related criminal cases that were open in that region.[104]

The Stone Line, FISA, and the Levi Guidelines all had profound implications for how domestic intelligence was practiced, governed, and conceptualized in the pre-9/11 era. Significantly, they all shared an (implicit) commitment to what it was that intelligence governance was fundamentally about: namely, warding off abuse. In other words, the governance mechanisms put in place by these reforms were not aimed at producing more effective or more rigorous intelligence. Rather, they sought to produce more legally compliant intelligence. They accomplished that objective by essentially employing a governance regime that opposed domestic intelligence by drawing on the assumptions and tools of criminal law.

2. The Criminal Standard and the Logic of Domestic Intelligence

The imposition of the conceptual framework of the criminal process on domestic intelligence agencies was not solely the result of a desire to vindicate civil liberties against a dangerous government power. Recourse to the criminal standard also reflected a perfectly understandable (if ultimately misguided) attempt to grapple with the deep meaning of domestic intelligence. As Richard Posner has observed, it is "the grip of our legalistic culture[] which makes us think that the regulation of national

> that the FBI shall use certain intrusive techniques only where it or the Attorney General or a court finds reasonable suspicion or probable cause that a criminal enterprise is underway. . . . If we are to apply the rule of law effectively to the exercise of investigative powers, our thinking must go beyond the criminal laws and beyond procedures linked to the criminal law by such shorthand terms as reasonable suspicion or probable cause. The FBI has been told what it should not do—that is, investigate without reasonable suspicion of criminal activity—but it has not been told what it should concentrate on doing. There must be a more systematic and principled analysis of where and why domestic security and foreign counterintelligence investigations are necessary.

ELLIFF, *supra* note 91, at 35.

104. Press Release, U.S. Dep't of Justice, Briefing with Department Officials on Consolidated Attorney General Guidelines (Sept. 13, 2008), *available at* http://justice.gov/opa/pr/2008/September/08-opa-814.html.

security *must* be modeled on the regulation of criminal law enforcement."[105] In some ways, it is easy to understand why: On the surface, intelligence gathering bears more than a passing resemblance to criminal investigation. It employs many of the same tools, from physical surveillance to confidential informants to electronic eavesdropping. Further, domestic intelligence is chiefly practiced, at least in the United States, by law enforcement agencies otherwise preoccupied with the investigation of crime. Indeed, the law enforcement culture of an agency like the FBI, which has historically rewarded agents who "make" criminal cases rather than those who participate in the more ineffable processes characteristic of intelligence gathering and analysis, has tended to reinforce the criminal standard all the more.[106] The problem with analogizing intelligence to criminal investigation is that, while the tools they employ (and the agencies that employ them) may be the same, the underlying purposes of the two activities are quite different.[107] As I argue in Part III, regulatory law and practice supply a vastly better analogy.

III. DOMESTIC INTELLIGENCE AS RISK ASSESSMENT

It has proven easier to criticize the suitability of the criminal standard than to find a new conceptual model to fit the emergent preventive regime.[108] If domestic intelligence does not amount to a form of criminal investigation, then what is it, and what is the nature of the power that the

105. Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 259 (2008). As I go on to argue in the next part, the source of conceptual confusion is not necessarily the grip that our legalistic culture has on us so much as it is the unexamined assumption that criminal law, rather than administrative law, ought to be at the forefront of intelligence governance.

106. *See* AMY B. ZEGART, SPYING BLIND: THE CIA, THE FBI, AND THE ORIGINS OF 9/11, at 121–27 (2007). *See also id.* at 127–55 (examining the intelligence failures by the FBI in the lead-up to 9/11 and criticizing as inadequate attempts to address these problems).

107. The Supreme Court has recognized a similar distinction when it comes to the constitutionality of roadblocks under the Fourth Amendment. Suspicionless stops that are motivated primarily by concerns about highway safety and border integrity, rather than by a general interest in criminal investigation and prosecution, may pass muster under the Fourth Amendment. *Compare* United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (upholding the constitutionality of a vehicle checkpoint where suspicionless searches for illegal aliens were performed based, in part, on the checkpoint's border control function), *with* City of Indianapolis v. Edmond, 531 U.S. 32 (2000) (finding that an antinarcotics roadblock violated the Fourth Amendment on the grounds that its purpose was to enforce criminal law and therefore that some individualized suspicion was required). The Court's "primary purpose" test announced in *Edmond*, *see Edmond*, 531 U.S. at 40, (unwittingly) echoes a line of cases that interpreted and gave meaning to the FISA wall, *see, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

108. *See* SHULSKY & SCHMITT, *supra* note 86, at 156 ("Asserting the theoretical argument against the criminal standard for domestic security investigations is much easier than determining what could replace it.").

government exercises in this area? I argue that the post-9/11 domestic intelligence process is properly regarded as a form of risk assessment. Risk assessment is a methodology that, over the last quarter-century, has transformed the government's approach to regulation by providing a framework for identifying public risks and prioritizing regulatory action.[109] Although historically it has been closely associated with certain specialized disciplines, such as toxicology and the detection of threats posed by hazardous substances,[110] risk assessment is most fundamentally "a systematic approach to organizing and analyzing scientific knowledge and information for potentially hazardous activities."[111] Furthermore, risk assessment is concerned with the vulnerabilities present in the ambient environment, not merely the intensity or virulence of a particular "pathogen" (or, alternatively, a dangerous and infectious ideology), because "[n]either an infectious agent nor its host can exist in a system where external conditions are unsuitable."[112] Stated at a high level of generality, domestic intelligence (no different from other forms of risk assessment) is simply a means by which the state generates information that will inform its decisionmaking about the health and safety of its citizens.

Domestic intelligence is best thought of as a form of risk assessment in three important ways.[113] First, risk assessment is proactive: it seeks to identify and measure risk in order to address it before, not after, harm has been done. Second, risk assessment is aggregative: it seeks out a wide

109. *See supra* note 26.

110. *See, e.g.*, COMM'N ON LIFE SCIS., NAT'L RESEARCH COUNCIL, RISK ASSESSMENT IN THE FEDERAL GOVERNMENT: MANAGING THE PROCESS 3, 19–20 (1983) (commonly known as the "Red Book") (defining risk assessment as potentially entailing four major steps: hazard identification, dose-response assessment, exposure assessment, and risk characterization).

111. COMM'N ON LIFE SCIS., NAT'L RESEARCH COUNCIL, SCIENCE AND JUDGMENT IN RISK ASSESSMENT 4 (1994) [hereinafter SCIENCE AND JUDGMENT]. Although OIRA has gestured in the direction of providing some standardization across different types of risk assessments, "[i]t remains the case . . . that overseeing the uncertainty in risk assessments is largely outside its purview." Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 COLUM. L. REV. 1260, 1297 (2006).

112. Kevin D. Lafferty, Katherine F. Smith & Elizabeth M. P. Madin, *The Infectiousness of Terrorist Ideology: Insights from Ecology and Epidemiology*, *in* NATURAL SECURITY: A DARWINIAN APPROACH TO A DANGEROUS WORLD 186, 188 (Raphael D. Sagarin & Terence Taylor eds., 2008).

113. My argument that domestic intelligence resembles risk assessment is pitched at a high level of generality. Inevitably, in practice the analogy is imperfect, notably in the sense that intelligence-cum-risk-assessment threatens to interfere with basic rights in a way that risk assessments in the environmental context, for example, do not. That said, this problematic feature of intelligence is also present in public health surveillance. For a provocative theory that epidemiology can shed light on counterterrorism intelligence, see *id.* at 188–90. *See also* Paul Stares & Mona Yacoubian, Op-Ed, *Terrorism as Virus*, WASH. POST, Aug. 23, 2005, at A15.

range of data in order to measure the prevalence of a risky substance or activity in society. Third, risk assessment relies on careful scientific analysis of data.

A. RISK ASSESSMENT AND PROACTIVENESS

Regulatory activity is often oriented toward prevention.[114] Rather than wait for an environmental pollutant to give rise to a nuisance that sounds in tort, for example, the regulatory state treats it as a problem that can be addressed by a proactive government policy. If this characterization is true of regulatory processes in general, then it is especially so of risk assessment, which "provides a way to determine the amount of risk posed in a given situation, which can inform policy decisions regarding risk management."[115] The purpose of risk assessment is precisely to inform regulatory policy decisions down the line.

Domestic intelligence is similarly concerned with obtaining information proactively.[116] As the new *Attorney General's Guidelines* put it,

> the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur.[117]

---

114. *See* Steven Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357 (1984) (comparing a tort-based model and a regulation-based model for addressing risk).

115. Angelo, *supra* note 26, at 1559. *See also* SCIENCE AND JUDGMENT, *supra* note 111, at 28 ("*Risk management* is the term used to describe the process by which risk-assessment results are integrated with other information to make decisions about the need for, method of, and extent of risk reduction.").

116. The adoption of this approach in preemptive counterterrorism—from the prosecution of preemptive wars to the use of preemptive detention—has proved controversial. *See* Stern & Wiener, *supra* note 38, at 395.

117. ATTORNEY GEN.'S GUIDELINES, *supra* note 85, at 17. The absence of a need for criminal predication in order to commence and carry out a threat assessment was also brought out during a recent colloquy between Senator Jay Rockefeller and FBI General Counsel Valerie Caproni. Senator Rockefeller asked whether the new guidelines authorized surveillance of "a law-abiding U.S. citizen or a permanent resident all day or for many days without grounds to believe that the person followed is engaged in activities that endanger the national security." The FBI General Counsel replied that "[i]t could." *Attorney General Guidelines for FBI Criminal Investigations, National Security Investigations, and the Collection of Foreign Intelligence: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 16 (2008) [hereinafter *Attorney General Guidelines Hearing*] (testimony of Valerie Caproni, General Counsel, FBI), *available at* http://intelligence.senate.gov/pdfs/110846.pdf. In another colloquy with Senator Russ Feingold, Caproni explained that while criminal predication was not necessary to carry out a threat assessment, the FBI "would only be collecting information if there is an authorized

The rationale here is simple: because of their potentially catastrophic impact, the government cannot allow the planning of certain terrorist attacks to go uninterrupted because they were not detected.[118] In explaining the practical import of the new guidelines, an FBI official offered the following advice to field agents, deliberately drawing a distinction between gathering intelligence and operations under the criminal standard: "Don't tell me how many cases you have. Go out and find out whether the threat is present."[119] It is unsurprising that the guidelines refer to this proactive authority as "threat assessment," perhaps unwittingly echoing the language and methodological assumptions of risk assessment.[120]

To claim that the risk-assessment framework entails proactive intelligence gathering is not necessarily to endorse all preemptive intelligence gathering vis-à-vis individuals, still less to sanction preemptive interventions in the name of counterterrorism. As to the first point, an analogy to public health may be illuminating. The risk-assessment model of

---

purpose . . . legitimately within the parameters of [the threat] assessment." *Id.* at 30 (testimony of Valerie Caproni, General Counsel, FBI).

118. *See* William C. Banks & M. E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 7 (2000) (noting that while criminal law generally takes aim at social evils that "primarily harm[] individuals," domestic intelligence seeks to anticipate broader and graver threats that "strike[] at the very foundation of . . . society" and thus that it is "increasingly doubtful that a remedy that regulates criminal investigations will adequately serve similar objectives in national security investigations" (footnotes omitted)).

119. Press Release, *supra* note 104 (quoting a senior FBI official's statement regarding the proposed ATTORNEY GENERAL'S GUIDELINES). The FBI official's observation followed this insight:

> To be an intelligence-driven agency, what we need to do is to be asking questions. What is the threat within your environment? . . . So let's say, today or a year ago or two years ago, if the question was asked of a special agent in charge of an FBI field office, "Do you have a problem of theft of high technology and theft of classified information within your domain?" Their answer would be, "Our Chinese squad has three cases against Chinese nationals." Okay, so we've got a little bitty problem. And some other SAC would say[,] "We've got 50 cases." So they've got a bigger problem.
>
> Wrong. One has three cases, one has 50 cases. You don't have a clue the size of the problem in either office, because they could be missing things. Right? Because they have to have something to open the case, but if . . . nobody tells them anything, they don't have the predication necessary to open the case, so they don't know they've got a threat.

Id. (quoting a senior FBI official's statement regarding the proposed ATTORNEY GENERAL'S GUIDELINES).

120. The new guidelines explicitly empower the FBI to

> develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI's responsibilities . . . . The[se] overviews and analyses . . . may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them.

ATTORNEY GEN.'S GUIDELINES, *supra* note 85, at 29. Furthermore, "[t]he FBI is authorized to conduct research, analyze information, and prepare reports and assessments concerning matters relevant to authorized FBI activities." *Id. Cf.* SECOND SPECIAL SENATE COMM. ON TERRORISM & PUB. SAFETY, CAN., TERRORISM 41 tbl. (1989) (showing that Canada's dedicated domestic intelligence service CSIS "is not oriented towards gathering evidence to support criminal prosecutions. CSIS' purpose is essentially intelligence and information gathering for risk assessment").

domestic intelligence is analogous to "disease surveillance," a standard feature of epidemiology.[121] The government enjoys greater latitude (and concerns for individual rights are relatively diminished) when anonymous data are studied for their health implications for an entire population. For example, when Google recently started tracking flu trends (by reference to searches for certain key words such as "influenza symptoms"), it committed to protecting individual privacy by making public (and retaining internally) only aggregate data.[122] So too, domestic intelligence as risk assessment poses a diminished threat to individual liberty because it focuses on identifying larger social trends rather than patterns of individual behavior.[123]

As for the latter critique, proactive intelligence is not the same as what Jules Lobel calls the "preventive paradigm" in counterterrorism, which, he argues, runs the risk of prioritizing "open-ended standards . . . over clear rules" and "suspicion" over "objective evidence."[124] Animating Lobel's

121. *See* Lafferty et al., *supra* note 112, at 188–90 (discussing how to apply health surveillance techniques as a method for combating risks associated with contracting the disease in question—in the case of counterterrorism efforts, the danger of the spread of a harmful ideology). *See also* Gail R. Janes et al., *Descriptive Epidemiology: Analyzing and Interpreting Surveillance Data*, *in* PRINCIPLES AND PRACTICE OF PUBLIC HEALTH SURVEILLANCE 112 (Steven M. Teutsch & R. Elliot Churchill eds., 2d ed. 2000); Denise Koo & R. Gibson Parish II, *The Changing Health-Care Information Infrastructure in the United States: Opportunity for a New Approach to Public Health Surveillance*, *in* PRINCIPLES AND PRACTICE OF PUBLIC HEALTH SURVEILLANCE, *supra*, at 76; Raul A Romaguera, Robert R. German & Douglass N. Klaucke, *Evaluating Public Health Surveillance*, *in* PRINCIPLES AND PRACTICE OF PUBLIC HEALTH SURVEILLANCE, *supra*, at 176; Stares & Yacoubian, *supra* note 113.

122. *See* Google.org, Flu Trends: How Does This Work?, http://www.google.org/about/flutrends/how.html (last visited Mar. 1, 2010) ("Google Flu Trends uses aggregated Google search data to estimate current flu activity around the world in near real-time."). *See also* Posting of the Editorial Board to the Board, http://theboard.blogs.nytimes.com/2008/11/12/google-flu-trends-when-the-government-knows-youre-sick/ (Nov. 12, 2008, 11:56 EST) ("Google says that Google Flu Trends will protect people's privacy by providing only aggregate data. That's true up to a point. If you and your neighbors all do searches for flu-related symptoms, you might be tipping the government off that you are a problem area. That aggregated data could conceivably lead the government to take 'control measures,' like a quarantine, aimed at your area.").

123. By analogy to Kenneth Culp Davis's famous dichotomy in administrative law, the intelligence being sought more closely resembles legislative facts than adjudicative facts. *See* 2 KENNETH CULP DAVIS & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE § 10.5 (3d ed. 1994). That said, it is true that risk assessments may be conducted on a more tactical level. *See, e.g.*, Henry H. Willis, *Using Risk Analysis to Inform Intelligence Analysis* 2 (RAND Infrastructure, Safety & Env't Working Paper Series, Paper No. WR-464-ISE, 2007), *available at* http://www.rand.org/pubs/working_papers/WR464/. In general, as tactical risk assessments become more focused on individuals (rather than on potentially vulnerable pieces of infrastructure), higher standards of due process may be triggered.

124. Jules Lobel, *The Preventive Paradigm and the Perils of Ad Hoc Balancing*, 91 MINN. L. REV. 1407, 1407, 1414, 1424 (2007). Attorney General John Ashcroft also termed this approach the "paradigm of prevention." *Id.* at 1407.

critique is his conviction that "odds-making" of the sort that is necessary in a risk-regulatory framework "is an inherently speculative enterprise."[125] Simply stated, there is a sharp distinction between the intelligence gathered under the regulatory paradigm—the risk assessment itself—and the more concrete and potentially rights-infringing uses to which some of that information might be put.[126] The regulatory paradigm of domestic intelligence that this Article describes and develops does not purport to govern the manner in which the government may choose to intervene in the lives of individuals suspected of participation in a terrorist plot, only the way in which the government may develop a picture of the threat.[127] Individualized due process of a much more substantial variety than that which is assumed under the model of domestic intelligence as risk assessment would be required before the state could arrest, detain, or deprive citizens of their property on the ground that they pose some threat of terrorist violence.[128]

---

125. *Id.* at 1418. *See also* Kate Martin, *Domestic Intelligence and Civil Liberties*, SAIS REV., Winter-Spring 2004, at 7, 13 (drawing attention to the "disturbing specter" of a proactive approach to intelligence bound up with aggressive intervention, including predator strikes, renditions, and indefinite detentions).

126. Not only does the risk-assessment model not furnish the basis for unchecked preemptive interventions, it may actually reduce the (perceived) need for preemptive interventions. It may be, in other words, that the more comprehensive a risk assessment, the less likely that the government is to feel compelled to intervene because of a sense of uncertainty about the underlying risk. It is useful to recall in this regard that J. Edgar Hoover opposed the internment of Japanese-Americans during World War II, believing the intelligence capabilities of the FBI to be sufficient to locate any risk that might emerge from that community without recourse to a strategy of mass detention. The matter was discussed as part of a colloquy surrounding the passage of the so-called Non-Detention Act. A sponsor of the Act, Congressman Thomas Railsback, reminded an opponent of the bill, Congressman Richard Howard Ichord, that "J. Edgar Hoover was opposed to detention camps, because he thought he had sufficient personnel to keep all these potential saboteurs under surveillance, and that they could prosecute the guilty in accordance with due process . . . ." 117 CONG. REC. H31,552 (daily ed. Sept. 13, 1971).

127. In addition to the distinction between intelligence as risk assessment and interventions, I would insist on carefully drawn "use restrictions" on information learned as part of a domestic intelligence program to see to it that, as Ben Wittes has put it, "[w]hat happens in counterterrorism stays in counterterrorism." *See* BENJAMIN WITTES, LAW AND THE LONG WAR: THE FUTURE OF JUSTICE IN THE AGE OF TERROR 252 (2008).

128. *Cf.* Richard A. Clarke, *Targeting Terrorists*, WALL ST. J., July 18, 2009, at W1 (recommending that the CIA focus on intelligence gathering and analysis and not be "tied to, prejudiced by, [or] . . . tainted with a connection to covert action"). The distinction I draw between risk assessment and interventions is consistent with the practice of domestic intelligence agencies in the United Kingdom, France, Canada, and Australia, none of which possesses the power of arrest or detention. *See* PETER CHALK & WILLIAM ROSENAU, CONFRONTING THE "ENEMY WITHIN": SECURITY INTELLIGENCE, THE POLICE, AND COUNTERTERRORISM IN FOUR DEMOCRACIES, at xii (2004) (describing the domestic intelligence agencies in the United Kingdom, France, Canada, and Australia).

B. RISK ASSESSMENT AND AGGREGATION

Not only does the risk-assessment model commit domestic intelligence to proactive gathering and analysis of intelligence, it necessarily entails broad-gauged surveillance.[129] Risk assessment does not proceed by studying the actual harmful effects of a toxin on one individual; it studies the incidence and potential effects of a toxin on an entire population.[130] Similarly, domestic intelligence as risk assessment inevitably casts a much wider net than domestic intelligence under the criminal standard, acquiring and making sense of large quantities of data about the world as part of what I call the aggregative feature of domestic intelligence.[131]

Aggregative data may prove useful in locating a known individual subject—for example, by allowing large quantities of information to be "mined" with sophisticated algorithms. Something like this process appears to have been on the mind of FBI director Robert Mueller when he spoke of

---

129. To say that risk assessment seeks aggregative data is not to suggest that domestic intelligence is or ought to be indiscriminate in the information it seeks. As I argue below, a mature governance regime employing rationality review can help police avoid the tendency of intelligence to confuse the need for aggregative data with the need to cast an ever-wider intelligence net.

130. *Cf.* Wendy K. Mariner, *Medicine and Public Health: Crossing Legal Boundaries*, 10 J. HEALTH CARE L. & POL'Y 121 (2007) (comparing public health to individualized medical care).

131. The risk-assessment model moves domestic intelligence in the direction of "positive intelligence," which Sherman Kent defines as "all the things you should know in advance of initiating a course of action." SHERMAN KENT, STRATEGIC INTELLIGENCE FOR AMERICAN WORLD POLICY 210 (1949). Kent distinguishes between "positive intelligence" and "security intelligence," which he defines as "the intelligence behind the police function." *Id.* at 209. He captures the difference between the two forms of intelligence by reference to an example:

> A policeman, alerted by security intelligence, will protect your house against burglars, or, if the house is robbed, he will use security intelligence to catch the burglars. But this policeman will not warn you when there is to be a boost in the price of beef, nor will he tell you when your bank is going to fail. This is not his job. To get this kind of protective knowledge, you will have to patronize some sort of positive intelligence service.

Id. at 211. My contention is that domestic intelligence has emerged as a form of positive intelligence, having been limited to security intelligence status during the previous generation.

Kent is closely associated with the perspective that intelligence collection and analysis ought to be hermetically sealed off from one another, a view that was institutionalized in the form of the sharp divide between the CIA's directorates of intelligence and operations. This account has been criticized recently. *See, e.g.*, PHILIP BOBBITT, TERROR AND CONSENT: THE WARS FOR THE TWENTY-FIRST CENTURY 333–35 (2008) (arguing against Kent's excessively scientistic conception of intelligence). *See also* DICKEY, *supra* note 20, at 148–49 (quoting a senior NYPD official as stating, "You don't have that in other intelligence agencies[—] . . . where the analysts and operators work side by side"). While these criticisms have a great deal of force in practice, Kent is surely correct that it makes sense to distinguish between what he calls a "surveillance operation," or the "ways by which the contemporary world is put under close and systematic observation," and a "research operation," or the "attempts to establish meaningful patterns out of what was observed in the past and attempts to get meaning out of what appears to be going on now." KENT, *supra*, at 4 (emphases omitted). Both are part of domestic intelligence as risk assessment.

"integrating [the FBI] in the intelligence community, and understanding that our task is to find that Mohamed Atta, who may be swimming in the oceans of 300,000 Americans, before that individual can undertake an attack."[132] But aggregative data are not necessarily acquired and evaluated in order to find the proverbial needle in a haystack; rather, the purpose may be to take measure of the haystack itself.

Broadly speaking, this is accomplished in one of two ways. Aggregative intelligence may be achieved through forms of network analysis: application of algorithms to large bodies of data to generate patterns that reveal potential threats.[133] The goal here is not to monitor the contents of electronic communications so much as to use the patterns of those communications as the basis for filling out a highly detailed account of social relations.[134] Combining network theory and high-power computing paves the way for "calculat[ing] to what extent elements are connected to other elements within a network . . . [and] measur[ing] . . . the quantitative relationship between the parts and the whole."[135]

To be certain, the effectiveness of data mining of this sort remains deeply contested.[136] So too does the legality of certain approaches to data

---

132. Robert S. Mueller III, Dir., FBI, Speech at the National Press Club (May 16, 2008) (transcript available at http://www.fbi.gov/pressrel/speeches/mueller051608.htm).

133. *See, e.g.*, PROTECTING INDIVIDUAL PRIVACY, *supra* note 56, at 241 (noting that TIA was intended to "develop technology that could discern event and transaction patterns of interest and *then* identify individuals of interest on the basis of the events and transactions in which they participated"). In a hearing focused on modernizing FISA, Senator Russ Feingold had a dialogue with Director of National Intelligence J. Michael McConnell, during which Feingold reminded McConnell that he had previously commented to the House Intelligence Committee that "the bulk collection of all communication originating overseas . . . 'would certainly be desirable if it was physically possible to do so,' but that bulk collection of communications with Americans is not needed." *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing on S. 1927 Before the S. Comm. on the Judiciary*, 110th Cong. 32 (2007) (testimony of Admiral J. Michael McConnell, Director of National Intelligence). Feingold proceeded to ask McConnell whether "bulk collection of all communications originating overseas, including communications of people in the United States" was '"authorized by the [new FISA law],"' to which McConnell responded that it would be authorized "[s]o long as it is foreign, in a foreign country for foreign intelligence purposes." *Id.* at 32–33 (testimony of Admiral J. Michael McConnell, Director of National Intelligence).

134. *See supra* Part II.A.3. Recall that the Supreme Court has held that the Fourth Amendment does not protect individuals against the disclosure of information that has been turned over to third parties. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301(a), 100 Stat. 1848, 1868–72; United States v. Miller, 425 U.S. 435 (1976), *superseded in part*, Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697.

135. *See* Ferenc Jordán, *Network Analysis Links Parts to the Whole*, *in* NATURAL SECURITY, *supra* note 112, at 240, 240.

136. *See* PROTECTING INDIVIDUAL PRIVACY, *supra* note 56, at 46 (proposing a framework for evaluating intelligence programs that asks two sets of questions: "First, is an information-based

mining. For example, an aggregative program seems to have been at the heart of the controversy that led to the famous showdown between government lawyers by John Ashcroft's hospital bed. According to a recent media report, "[T]he clash erupted over a part of Bush's espionage program that had nothing to do with the wiretapping of individual suspects. Rather, Comey and others threatened to resign because of the vast and indiscriminate collection of communications data."[137] In collaboration with major telecommunications firms, the NSA had acquired records of calls and emails—so-called metadata, which lacked the contents of the communication—and analyzed the information for patterns potentially suggestive of terrorist activity.[138]

Attempting to take measure of large groups in order to detect the presence of a threat is not limited to the world of supercomputing and metadata; increasingly, this type of aggregative intelligence is also achieved by a form of human intelligence, where social-scientific techniques are applied to understand potentially relevant phenomena in a defined population.[139] Counterterrorism intelligence has come to rely on "thick description"[140] of social phenomena as an important risk-assessment tool, employing various means of human intelligence to develop an understanding of larger social trends.[141] The purpose and scope of this sort of intelligence gathering is captured by a British intelligence initiative called "Rich Picture." Rich Picture was designed over the last two years to gather intelligence at the local level "to allow [the security apparatus] to understand the make-up and dynamics of local communities, where

program effective or likely to be effective in achieving its intended goal—in short, does it work? Second, does the program comply with the law and reflect the values of society, especially concerning the protection of data subjects' civil liberties?").

137. Klaidman, *supra* note 6.

138. A recent report suggests that the NSA has recently stopped collecting certain metadata in response to concerns raised by members of the FISC. *See* Ellen Nakashima, *NSA Stops Collecting Some Data: Officials Trying to Resolve Concerns Raised by Court*, WASH. POST, Apr. 19, 2010, at A6.

139. *Cf.* CLIFFORD GEETRZ, *Thick Description: Toward an Interpretive Theory of Culture*, *in* THE INTERPRETATION OF CULTURES 3 (1973) (examining the application of this type of technique in cultural anthropology). In some cases, interviewing one individual may give rise to a great deal of strategically valuable intelligence. *See* MORGAN, *supra* note 62, at 93 (stating that the use of undercover officers and paid informants is "the most productive means of gathering intelligence information"). To generalize from this observation, not all aggregative intelligence is strategic (as when volumes of information are analyzed to turn up a trace of a known subject), and not all strategically valuable intelligence is aggregative.

140. The term famously belongs to Clifford Geertz. *See generally* GEERTZ, *supra* note 139.

141. In the intelligence context, for example, a paid undercover informant can serve a valuable function as a "vacuum cleaner of information." *See* MORGAN, *supra* note 62, at 93 (quoting a Church Committee finding).

radicalization could occur, and identify individuals of authority and influence within the community."[142] Rich Picture, in other words, is a form of official sociology whereby the police and intelligence services develop insights into the cultural and economic landscape of neighborhoods and communities.

The FBI has recently undertaken its own version of Rich Picture, which the FBI refers to as "domain management." Like Rich Picture, domain management is rooted in an anthropological approach to intelligence. It seeks to gather information and generate analyses of pertinent social phenomena taking place in the domains within which agents operate. As FBI director Mueller explained it, "The goal of domain management is to develop a comprehensive understanding of a territory's threats and vulnerabilities so that managers can effectively deploy resources for greatest impact."[143] The brainchild of a former CIA analyst,

142. BRITISH HOME OFFICE, APACS TECHNICAL CONSULTATION: SERIOUS CRIME AND PROTECTION 50 (2007), *available at* http://police.homeoffice.gov.uk/publications/police-reform/2007-12-07_APACS_Technical_52835.pdf?view=Binary (defining "Rich Picture" in a template for receiving performance data). *See also* HM GOV'T, THE UNITED KINGDOM'S STRATEGY FOR COUNTERING INTERNATIONAL TERRORISM 65 (2009), *available at* http://security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/ ("Under [Rich Picture,] information is collected on issues related to violent extremist activity in local communities."). Settling on the correct unit of analysis for Rich Picture may be challenging. First of all, at the conceptual level, "[t]he global Salafi jihad has a very fuzzy boundary . . . [which] raises . . . epistemological issues on a group and individual level." MARK SAGEMAN, UNDERSTANDING TERROR NETWORKS 151 (2004). Furthermore, the nature of the current threat mandates a reconsideration of the familiar distinctions between domestic and overseas threats. As NYPD deputy commissioner for counterterrorism Richard Falkenrath has observed, "Despite the success of U.S. overseas efforts in degrading al-Qaeda as an organization, its powerful radical influence on the City's younger generation—especially among its sizeable Muslim community—continues to pose a serious threat from within." POSNER, *supra* note 32, at 146. The debate about the viability of the foreign/domestic distinction in national security threats has been going on for over a generation. *See, e.g.*, Lewis F. Powell, Jr., *Civil Liberties Repression: Fact or Fiction?—"Law-Abiding Citizens Have Nothing to Fear,"* RICH. TIMES-DISPATCH, Aug. 1, 1971, *reprinted in Nominations of William H. Rehnquist and Lewis F. Powell, Jr.: Hearings Before the S. Comm. on the Judiciary*, 92d Cong. 213–14 (1971) (observing that "[t]here may have been a time when a valid distinction existed between external and internal threats" but that "such a distinction is now largely meaningless"). It is ironic that Justice Powell shortly thereafter authored the Court's opinion in *Keith*, in which precisely the foreign/domestic distinction was found to be of the essence. *See* Trevor W. Morrison, *The Story of* United States v. United States District Court *(*Keith*): The Surveillance Power*, *in* PRESIDENTIAL POWER STORIES 287, 317 (Christopher H. Schroeder & Curtis A. Bradley eds., 2009) (offering different explanations for Justice Powell's apparent shift).

There has already been the suggestion in congressional testimony that the FBI engages in this sort of surveillance more vigorously in certain communities than others. As Senator Feingold observed in a recent hearing, a senior FBI official made specific reference to collecting intelligence in Dearborn, Michigan, "which, of course, has a large Arab-American and Muslim community." *Attorney General Guidelines Hearing*, *supra* note 117, at 30 (testimony of Valerie Caproni, General Counsel, FBI).

143. Robert S. Mueller III, Dir., FBI, Statement at the Hearing Before the Subcommittee on Science of the House Committee on Appropriations, the Departments of State, Justice, and Commerce,

domain management was debuted at a meeting in February 2006 where FBI agents were shown "a map of the San Francisco area, pocked with data showing where Iranian immigrants were clustered."[144] This sort of demographic detail ostensibly allowed FBI agents to develop an assessment of the threat emanating from a certain community.[145] As in the case of data mining, however, questions about the effectiveness and legality of such programs remain,[146] especially because programs of this sort currently elude meaningful intelligence governance.

C. RISK ASSESSMENT AND ANALYSIS

The risk-assessment approach to domestic intelligence not only entails proactive, aggregative collection, but also demands rigorous scientific analysis of the data that have been acquired. As Richard Betts has written, "Threat assessment poses two tasks: collecting facts and interpreting their implications."[147] The risk-assessment model helps clarify that "[a]nalysis . . . is part of a scientific process"[148] and that "[i]ntelligence analysis can be reconstructed in the context of a scientific method" to include "observation and description of phenomena; formulation of hypotheses to explain phenomena; testing of hypotheses by independent experts; [and] refutation or confirmation of hypotheses."[149] Historically, the role of analysis has not received the attention it deserves within the FBI[150]—a classic manifestation of a larger phenomenon that for those "who

---

and Related Agencies of the 109th Congress (Sept. 14, 2006) (transcript available at http://www.fbi.gov/congress/congress06/mueller091406.htm).

144. Scott Shane & Lowell Bergman, *F.B.I. Struggling to Reinvent Itself to Fight Terror*, N.Y. TIMES, Oct. 10, 2006, at A6.

145. As Amy Zegart has reportedly stated, "Domain management has been portrayed by the bureau as a broad analytic approach, not specific data mining activities. . . . It is a methodology to determine what is known about a problem, develop indices to measure it, and take steps to close knowledge gaps." Jeff Stein, *FBI Hoped to Follow Falafel Trail to Iranian Terrorists Here*, CQ POL., Nov. 2, 2007, http://www.cqpolitics.com/wmspage.cfm?docID=hsnews-000002620892. As part of the project, it was reported that "the FBI sifted through customer data collected by San Francisco-area grocery stores in 2005 and 2006, hoping that sales records of Middle Eastern food would lead to Iranian terrorists." *Id.*

146. *Id.* (stating, with regards to domain management's ability to estimate the number of Hamas or Hezbollah members in the United States, "[W]ho knows?").

147. RICHARD K. BETTS, ENEMIES OF INTELLIGENCE: KNOWLEDGE AND POWER IN AMERICAN NATIONAL SECURITY 54 (2007).

148. ROB JOHNSTON, CIA, ANALYTIC CULTURE IN THE U.S. INTELLIGENCE COMMUNITY: AN ETHNOGRAPHIC STUDY 17 (2005), *available at* http://www.fas.org/irp/cia/product/analytic.pdf (emphasis omitted).

149. *Id.* at 19.

150. *See, e.g.*, *id.* at 43 ("The practice of medicine has been revolutionized by the sciences that underpin its workings. Intelligence analysis has not experienced that revolution. Unlike medicine, the

are primarily interested in 'making cases,' anything which smacks of research or intelligence is afforded low status within the organisation."[151]

Sound analysis depends on the availability of valid theories for making sense of—and prioritizing—the information that has been acquired. As David Omand has put it, "The value of a strategic intelligence judgment, like a scientific theory, lies in its explanatory power, and thus its predictive power."[152] Such a theory might, for example, take the form of a social scientific account of radicalization that purports to elaborate the production cycle for terrorists and the terrorist threat. Radicalization that may culminate in terrorist violence inevitably takes place within a thick social context, with various institutions, groups, and communities—real and virtual—playing a part.[153] As a result, risk assessment must concern itself with understanding "the foundations on which a culture's education, religion, media, legislation, and ideology are set."[154] It is of course the case that theories and analytic conclusions of this sort can miss the mark or prove to be of limited value,[155] a problem that can be especially acute in the

basic sciences that underpin intelligence are the human sciences, which are considerably more multivariate and more difficult to control."); Shane & Bergman, *supra* note 144 (stating that "FBI culture still respects door-kicking investigators more than desk-bound analysts sifting through tidbits of data"); Gregory F. Treverton, *Risk and Riddles: The Soviet Union Was a Puzzle, Al Qaeda Is a Mystery, Why We Need to Know the Difference*, SMITHSONIAN, June 2007, at 98 ("Th[e] change in mission [from law enforcement to intelligence] requires an enormous change in organizational culture. For the puzzles of law enforcement, the measures of effectiveness are pretty clear—you can count the suspects collared and bad guys convicted. Terrorists, however, may commit but one crime, and by the time they do, it is too late. That scarcity of 'collars' is a main reason why, rhetoric aside, counterterrorism was not a marquee FBI mission before 9/11."). *See generally* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF JUSTICE, AUDIT REPORT 07-30, FOLLOW-UP AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO HIRE, TRAIN, AND RETAIN INTELLIGENCE ANALYSTS (2007) (discussing how the FBI has made improvements in the analysis of intelligence and making recommendations for further improvements). A 2008 memorandum for heads of departments states that "[f]urther enhancement of the FBI's intelligence analysis capabilities and functions has been recognized consistently as a key priority in the legislative and administrative reform efforts following the September 11, 2001, terrorist attacks." Memorandum from the Attorney Gen. to the Heads of Dep't Components 3–4 (Sept. 29, 2008), *available at* http://www.usdoj.gov/ag/readingroom/guidelines-memo.pdf.

151. GILL, *supra* note 70, at 210 (footnote omitted).

152. David Omand, *Reflections on Secret Intelligence*, *in* THE NEW PROTECTIVE STATE: GOVERNMENT, INTELLIGENCE AND TERRORISM 97, 111 (Peter Hennessy ed., 2007).

153. *Cf.* Grodsky, *supra* note 26, at 177 (arguing that, in the context of assessing health risks to individuals with certain genetic predispositions, "society must decide when, in the continuum from exposure to disease, early indicators of future harm are sufficiently predictive to qualify as harms in themselves").

154. Lafferty et al., *supra* note 112, at 200 (citing terrorism expert Rohan Gunaratna).

155. Radicalization theory, for example—which posits that extremism results from moral feeling being transformed by social patterns—is in its intellectual infancy. *See* Cass R. Sunstein, *Misery and Company*, NEW REPUBLIC, Oct. 2, 2008, at 39 (reviewing MARC SAGEMAN, LEADERLESS JIHAD: TERROR NETWORKS IN THE TWENTY-FIRST CENTURY (2008)).

intelligence community where the felt need for secrecy inhibits the ability of officials to benefit from outside perspectives.

IV. REGULATORY INTELLIGENCE GOVERNANCE

To address the vacuum in domestic intelligence governance, we need to employ a regime that is suited to the activities and institutions that require governing. In view of the regulatory nature of domestic intelligence discussed above, I argue in this part that the basic features of administrative law—specifically a particularly expansive conception of cost-benefit analysis that I refer to as rationality review, (judicial) review for compliance with regulatory mandates, and pluralism underwritten by transparency—should assume a central role in the governance of domestic intelligence.

Regulatory governance would do more than leverage some of the basic concepts and tools of administrative law. It would, at the same time, redefine what it means to govern intelligence. Against a historical backdrop of narrowly drawn intelligence governance focused on the prevention of outright abuse or illegality, regulatory governance implies a robust framework that simultaneously aims to produce more accurate, more cost-effective, and more rights-protecting intelligence. Furthermore, and most consequentially, regulatory governance would pave the way for a renegotiation of what has been called the "social contract" between the people and the domestic intelligence apparatus.[156] Jody Freeman's observation, that "[s]ince the New Deal explosion of government agencies, administrative law has been defined by the crisis of legitimacy and the problem of agency discretion,"[157] is equally applicable to domestic intelligence. The governance framework I envision could serve as a means for restoring public trust—"a critical, but widely neglected, element in risk regulation"[158]—in domestic intelligence.

---

156. I owe this felicitous idea to veteran policymaker and intelligence expert Philip Zelikow.

157. Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 545–46 (2000) (footnote omitted).

158. *See* Richard H. Pildes & Cass R. Sunstein, *Reinventing the Regulatory State*, 62 U. CHI. L. REV. 1, 40 (1995) (arguing for the centrality of trust to effective administrative regulation). Pildes and Sunstein go on to suggest that

> Trust is important to the regulatory process in at least three ways. First, levels of trust shape public knowledge about risk. Second, levels of trust influence the ability of regulators to communicate effectively about risk. Finally, public trust is critical to public acceptance of regulatory proposals for dealing with risk.

Id. In the intelligence context, all three aspects of trust, in turn, depend on the ability of the intelligence apparatus to become more transparent, notwithstanding its powerful tendency to cloak itself in secrecy. *Id.*

A. RATIONALITY REVIEW

For a generation, a certain conception of rationality review, namely cost-benefit analysis, has dominated the regulatory state. Embodied in highly influential executive orders and regulatory statutes, and embraced by presidents of both parties,[159] cost-benefit analysis amounts most basically to the appealing idea that a proposed regulation ought to produce more social gain, in the aggregate, than harm.[160] Beyond this simple idea lurk myriad complexities. For one thing, scholars contest the exact nature of the cost-benefit calculus.[161] Some challenge the moral foundations of cost-benefit analysis.[162] Others have drawn attention to the ways in which cost-benefit analysis, as operationalized in the regulatory state, has

159. *See, e.g.*, Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993) (endorsing the essential features of Executive Order 12,291); Exec. Order No. 12,291, 46 Fed. Reg. 13,193 (Feb. 17, 1981). As for legislative initiatives accepting cost-benefit analysis, see, for example, the Toxic Substances Control Act, Pub. L. No. 94-469, § 6(a), 90 Stat. 2003, 2020–21 (1976) (codified as amended at 15 U.S.C. § 2605(a) (2006)) (authorizing administrative action if there is a "reasonable basis"), and the Federal Environmental Pesticide Control Act of 1972, Pub. L. No. 92-516, sec. 3, § 3, 86 Stat. 973, 979–82 (codified as amended at 7 U.S.C. § 136a(a) (2006)) (amending the Federal Insecticide, Fungicide, and Rodenticide Act of 1947) (authorizing administrative regulation to prevent "unreasonable adverse effects on the environment"). For a brief history of cost-benefit analysis in the regulatory state, see Robert W. Hahn & Cass R. Sunstein, *A New Executive Order for Improving Federal Regulation? Deeper and Wider Cost-Benefit Analysis*, 150 U. PA. L. REV. 1489, 1505–10 (2002).

160. Although cost-benefit analysis per se is frequently—and perhaps ideally—thought to consist of a pure comparison of monetized costs with monetized benefits, cost-benefit analysis can also be used to describe a comparison of heterogeneous values. *See* Richard A. Posner, *Cost Benefit Analysis: Definition, Justification, and Comment on Conference Papers*, 29 J. LEGAL STUD. 1153, 1153–56 (2000). I use rationality review throughout this discussion as shorthand to refer, not only to cost-benefit analysis itself, but also to other related methods of evaluating government policies or actions, such as risk-cost analysis and cost effectiveness. For an overview of these methods, as well as their challenges and limitations, see JOHN L. MOORE, CONG. RESEARCH SERV., REPORT NO. 95-760 ENR, COST-BENEFIT ANALYSIS: ISSUES IN ITS USE IN REGULATION (1995), *available at* http://ncseonline.org/NLE/CRSreports/Risk/rsk-4.cfm (describing some of the challenges to applying the cost-benefit analysis in a manner that is cost efficient and produces consistent results).

161. *See generally* MOORE, *supra* note 160; W. KIP VISCUSI, FATAL TRADEOFFS: PUBLIC AND PRIVATE RESPONSIBILITIES FOR RISK (1992) (discussing risk valuations, responses to the risk, and how best to regulate risk); RISK VERSUS RISK: TRADEOFFS IN PROTECTING HEALTH AND THE ENVIRONMENT (John D. Graham & Jonathan Baert Wiener eds., 1995) (presenting arguments for how to treat risk minimization holistically where measures to avoid risk entail risks of their own).

162. *See, e.g.*, Amartya Sen, *The Discipline of Cost-Benefit Analysis*, *in* COST-BENEFIT ANALYSIS: LEGAL, ECONOMIC, AND PHILOSOPHICAL PERSPECTIVES 95 (Matthew D. Adler & Eric A. Posner eds., 2000). As Sen notes, "It is indeed perfectly possible for someone to accept the foundational outlook of cost-benefit analysis and yet reject one or more of the requirements imposed by the structural demands, evaluative indifferences, and market-centered valuation that characterize [its] mainstream applications." *Id.* at 97. *See also* Martha C. Nussbaum, *The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis*, *in* COST-BENEFIT ANALYSIS, *supra*, at 169, 193 (noting the dangers of how costs and benefits are weighted under a "willingness-to-pay model" and "defin[ing] cost-benefit analysis in a way that does not entail any particular way of assigning the weightings").

historically been prone to various ideological, cognitive, and institutional biases.[163] Contested though it is in theory and in practice, cost-benefit analysis is "here to stay" in the regulatory state[164]—including, as of late, some portions of the regulatory state concerned with issues of national security.[165]

Cost-benefit analysis narrowly defined, however, does not exhaust the possibilities of rationality review. Not only does rationality review entail the possibility of different quantitative methods, such as cost effectiveness,[166] it also includes, more generally, the balancing of competing interests rooted in security and liberty.[167] In this respect, rationality review addresses a set of conceptual and practical challenges that stem from the tendency of a certain narrow conception of cost-benefit analysis to assign strict monetary values to terrorism risk,[168] as well as to

163. For an analysis by supporters of cost-benefit analysis who criticize how it has been operationalized, see RICHARD L. REVESZ & MICHAEL A. LIVERMORE, RETAKING RATIONALITY 9–51 (2008) (arguing that policymakers should redeem cost-benefit analysis from its historical antiregulatory applications). *See also* Pildes & Sunstein, *supra* note 158, at 43–48. Cost-benefit detractors point to some of the same biases in application as evidence that cost-benefit analysis itself is inherently flawed. *See, e.g.*, David M. Driesen, *Is Cost-Benefit Analysis Neutral?*, 77 U. COLO. L. REV. 335 (2006).

164. REVESZ & LIVERMORE, *supra* note 163, at 11.

165. Pursuant to Executive Order 12,866, DHS security regulations with an economic impact greater than $100 million are subject to OMB review. *See* Scott Farrow & Stuart Shapiro, *The Benefit-Cost Analysis of Security Focused Regulations*, 6 J. HOMELAND SECURITY & EMERGENCY MGMT. 1, 2 (2009). *See also* JOHN MOTEFF, CONG. RESEARCH SERV., REPORT NO. RL32561, RISK MANAGEMENT AND CRITICAL INFRASTRUCTURE PROTECTION: ASSESSING, INTEGRATING, AND MANAGING THREATS, VULNERABILITIES AND CONSEQUENCES (2005) (discussing the use of risk assessment in statutorily mandated DHS decisions of how to protect national infrastructure).

166. Brian A. Jackson, *Exploring the Utility for Considering Cost-Effectiveness Analysis of Domestic Intelligence Policy Change*, *in* THE CHALLENGE OF DOMESTIC INTELLIGENCE, *supra* note 39, at 205. *See also* MOORE, *supra* note 160.

167. *See* Exec. Order No. 12,866, 58 Fed. Reg. 51,735, 51,735 (Sept. 30, 1993) ("Costs and benefits shall be understood to include both quantifiable measures . . . and qualitative measures . . . ."); Jackson, *supra* note 166, at 205 ("[A] *qualitative* cost-benefit approach can be useful to discipline thinking and ensure that important policy effects are not being ignored . . . ."). *See also* HENRY H. WILLIS, RAND, CHALLENGES OF APPLYING RISK MANAGEMENT TO TERRORISM SECURITY POLICY 5 (2008), *available at* http://www.rand.org/pubs/testimonies/2008/RAND_CT310.pdf (entered into the record at a June 2008 hearing before a subcommittee of the House Homeland Security Committee, *see The Goodyear Explosion: Ensuring Our Nation is Secure by Developing a Risk Management Framework for Homeland Security: Hearing Before the Subcomm. on Transportation, Security, and Infrastructure Protection of the H. Comm. on Homeland Security*, 110th Cong. 3 (2008)) (arguing that "the notion of a cold, analytic, actuarial risk assessment is largely a myth").

168. A scientific literature has developed that is concerned with the measurement of low-probability, high-risk events. *See, e.g.*, B. JOHN GARRICK, QUANTIFYING AND CONTROLLING CATASTROPHIC RISKS (2008); RICHARD A. POSNER, CATASTROPHE: RISK AND RESPONSE (2004). Nevertheless, the use of rationality review for national security–related matters is a generation behind the science of rationality review with respect to environmental regulation, *see* Farrow & Shapiro, *supra* note 165, at 13, suggesting the need for more careful thought devoted to the issue and its application to

the invasion of civil liberties.[169]

Still, intelligence has thus far remained impervious to rationality review, including in the narrow sense of comparing monetized costs and benefits, at least to any systematic application of the discipline. Employing rationality review as a standard tool for proposed intelligence programs would represent an important development in the governance of intelligence in a number of respects. First, and most basically, rationality review would help promote more accurate and cost-effective intelligence. Second, and somewhat more controversially, I argue that rationality review may actually prove to be a more effective tool for the protection of basic rights than the current governance regime. Third, anticipating a discussion of the institutional landscape of domestic intelligence governance in Part V, I argue that rationality review will help supply the methodological foundations of a centralized regulatory review process in the intelligence sphere akin to the role that OIRA has come to play in the regulatory state. Significant for this Article's central claim about the nature of intelligence as a form of risk assessment, rationality review respects the defining features of intelligence: its state of being aggregative, analytical, and anticipatory.

1. Accurate Intelligence

Rationality review of intelligence programs may be conducive to more accurate intelligence in three significant ways. First, rationality review promises heightened scientific rigor in the intelligence process by revealing submerged analytic assumptions[170] and forcing intelligence officials to articulate rationales for preferring one course of action over another. Second, and relatedly, rationality review of intelligence raises consciousness of, and helps to combat, the role of heuristic biases and bureaucratic pathologies prevalent among intelligence professionals.[171] Third, rationality review functions as a potential bulwark against the politicization of intelligence, a notorious problem during the Cold War, as well as in more recent times.

---

the governance of intelligence. For an extremely rough attempt at calculating costs and benefits in terms of security and civil liberties, see W. Kip Viscusi & Richard J. Zeckhauser, *Sacrificing Civil Liberties to Reduce Terrorism Risks*, 26 J. RISK & UNCERTAINTY 99 (2003).

169. *See* Jackson, *supra* note 166, at 210–11.

170. *See* Pildes & Sunstein, *supra* note 158, at 72 (noting how, instead of using cost-benefit analysis in a vacuum, cost-benefit analysis should be used for regulatory purposes in conjunction with other tools, such as value judgments, to make it a more useful assessment tool).

171. *See* Hahn & Sunstein, *supra* note 159, at 1502 (explaining how cost-benefit analysis can be used to overcome emotional and cognitive limitations in understanding risks).

While a veneer of scientific rigor attends intelligence analysis—for example, intelligence estimates, especially those that involve "assigning precise numerical ratings," are frequently marked with levels of confidence ranging from "high probability" to "'cannot rule out'"[172]—intelligence has been surprisingly untouched by thorough risk-based analysis. As the anthropologist of intelligence Rob Johnston has lamented, intelligence officials "quite often use[] the word 'tradecraft' to describe intelligence analysis,"[173] a method that Johnston juxtaposes with "scientific process."[174] Rationality review takes aim at precisely this phenomenon and forces officials to move from inherently unreliable intuitionism to more rational methods of assessment and analysis.[175] As Amartya Sen has explained, "[E]xplicitness . . . present[s] some kind of . . . barrier against [the] implicit railroading of unacceptable decisions that would be widely rejected if properly articulated."[176]

Not only would rationality review play a role in rooting out the distorting influences of personal bias, it would perform a valuable function in addressing specific kinds of heuristic and institutional biases endemic to intelligence, which impede clear thinking about a threat and the best

172. POSNER, *supra* note 32, at 3 (quoting OFFICE OF DIR. OF NAT'L INTELLIGENCE, NATIONAL INTELLIGENCE ASSESSMENT: PROSPECTS FOR IRAQ'S STABILITY: A CHALLENGING ROAD AHEAD 4 (2007), *available at* http://dni.gov/press_releases/20070202_release.pdf).

173. JOHNSTON, *supra* note 148, at 17. As Johnston explains, "The notion that intelligence operations involve tradecraft, which I define as practiced skill in a trade or art, may be appropriate, but the analytic community's adoption of the concept to describe analysis and analytic methods is not." *Id.* (emphasis omitted).

174. *See id.* ("[A]nalysis is neither craft nor art.").

175. *See* REVESZ & LIVERMORE, *supra* note 163, at 13 ("Cost-benefit analysis can be used to ensure that [agencies'] decisions are based on reasoned analysis and not, for instance, on the unaccountable whim of an official . . . ."). The intuition of intelligence officials, no different from that of any other kind of official, reflects the particular biases derived from their specific training, bureaucratic position, and upbringing. In the words of Gordon Woo, one of the inventors of the "Terrorism Risk Model" used by insurance companies and the government, "Just as the intuition of environmentalists may not provide the best societal solutions to environmental protection, so the intuition of law enforcement personnel may not provide the best overall answer to homeland security." Gordon Woo, The Benefits and Costs of Homeland Security Rules: Comments Prepared for the Office of Management of Budget 1 (Mar. 2003) (unpublished manuscript, *available at* http://www.whitehouse.gov/omb/inforeg/2003report/15.pdf). One could say the same thing about intelligence officials. Moreover, the influence of intuition threatens to be particularly acute in the field of terrorism, due to the high degree of informational uncertainty. *See* Michael Fitzsimmons, *The Problem of Uncertainty in Strategic Planning*, SURVIVAL, Winter 2006–07, at 131, 132 ("The record of planning for post-war operations in Iraq . . . decision-makers, in enlisting uncertainty as a rationale for discounting one set of predictions, have fallen prey to overconfidence in their own alternative set of predictions.").

176. Sen, *supra* note 162, at 99.

approaches to tackling it.[177] One basic form of institutional bias (well documented in the case of intelligence analysis) is tunnel vision: the tendency of intelligence professionals to overstate the importance of addressing the full implications of risk A while risk B goes unattended to.[178] Tunnel vision may affect individual analysts, but it is just as likely to take root in whole organizations. For example, an intelligence agency (especially one that combines intelligence and law enforcement functions) may attempt to run all possible leads on a threatening individual or group without stopping to consider that other, potentially much more threatening, individuals may go undetected as a function of resource allocation.[179] Another worrisome heuristic bias is groupthink: the tendency of members of an organization to converge on an approach to a particular problem due to social pressure and convention rather than considered judgment.[180] Meanwhile, cognitive biases, such as probability neglect,[181] may frustrate attempts to assess accurately the nature of the threat (and, by implication, to select the precise tools needed to combat it).[182] A properly designed regime of rationality review[183] would filter for these biases, not only by drawing attention to their distorting influences, but also by directing intelligence agencies to address relatively unheralded problems.

Finally, rationality review would promote more accurate intelligence by locating and helping to weed out overtly politicized intelligence.[184]

---

177. An emerging literature discusses the role of cognitive bias in intelligence analysis. *See, e.g.*, Jack Davis, *Why Bad Things Happen to Good Analysts*, *in* ANALYZING INTELLIGENCE, ORIGINS, OBSTACLES, AND INNOVATIONS 157 (Roger Z. George & James B. Bruce eds., 2008); Richard J. Heuer, Jr., PSYCHOLOGY OF INTELLIGENCE ANALYSIS 121–75 (2006).

178. *See* STEPHEN BREYER, BREAKING THE VICIOUS CIRCLE: TOWARD EFFECTIVE RISK REGULATION 11–19 (1993). *See generally id.* (prescribing technocratic solutions to systematic problems of the administrative state).

179. *See, e.g.*, Eric Schmitt, *F.B.I. Agents' Role Is Transformed by Terror Fight*, N.Y. TIMES, Aug. 19, 2009, at A1 (quoting intelligence scholar Amy Zegart that in FBI counterterrorism units, "there's more chasing than assessing," suggesting a lack of strategic vision).

180. *See* IRVING L. JANIS, VICTIMS OF GROUPTHINK: A PSYCHOLOGICAL STUDY OF FOREIGN-POLICY DECISIONS AND FIASCOES 8–9 (1967) (describing three conceptual frameworks for how group dynamics affect U.S. foreign policy). *See also* Paul B. Paulus, *Developing Consensus About Groupthink After All These Years*, 73 ORG. BEHAV. & HUM. DECISION PROCESSES 362 (1998) (evaluating the development and status of the groupthink theory).

181. *See* Cass R. Sunstein, *Terrorism and Probability Neglect*, 26 J. RISK & UNCERTAINTY 121 (2003).

182. *See generally* Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, *in* JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 3, 11–14 (Daniel Kahneman, Paul Slovic & Amos Tversky eds., 1982) (noting several types of cognitive bias).

183. *See* REVESZ & LIVERMORE, *supra* note 163, at 9–19 (noting that a properly functioning cost-benefit analysis review process would actively draw attention to the areas where there is insufficient regulation, not merely those where there was ostensibly too much regulation).

184. For a compelling typology and analysis of politicization, see Gregory F. Treverton,

History teaches that the politicization of intelligence can be irresistible to some powerful public figures.[185] Whether intended to maximize political advantage by engaging in demagoguery of the terrorist threat or by spying on (and blackmailing) political foes, politicization threatens the integrity of the intelligence process itself. While it is possible that even a searching rationality review analysis will fail to take note of (or be able to handle) certain forms of politicization,[186] the rationality review process at a minimum gives a boost to the opponents of politicization by giving them a voice in a formal review process and creates the possibility of a neutral ground on which to resolve internal conflicts.

2. Rights-Protecting Intelligence

While rationality review is not vulnerable to the criticism lodged against narrower conceptions of cost-benefit analysis to the effect that they (inappropriately and inadequately) attempt to monetize all costs and benefits including those that correspond to basic rights,[187] it is potentially subject to the more general critique that it furnishes the basis for downplaying rights protection in the national security area.[188] But rationality review need not entail this bias against rights protection. As a theoretical matter, even cost-benefit analysis can operate under certain deontological constraints.[189] More practically, even a balancing regime

---

Intelligence Analysis: Between "Politicization" and Irrelevance, *in* ANALYZING INTELLIGENCE, *supra* note 177, at 91.

185. In the words of Secretary of Defense and former CIA director Robert Gates, "The problem of politicization is as old as the intelligence business." Robert M. Gates, Guarding Against Politicization, Remarks Made Before the CIA (Mar. 16, 1992), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v36i1a01p_0001.htm.

186. Indeed, rationality review may itself become the occasion for politicization, with politicians either trumpeting a conclusion with which they agree or casting aspersions on a rationality review determination as insufficiently attuned to the threat.

187. *See* Jackson, *supra* note 166, at 210–11, 214, 219, 222–24.

188. *See, e.g.*, ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY, AND THE COURTS 274 (2007) (questioning the civil libertarian impulse to engage in "sophisticated second-order arguments" to defeat claims of executive authority in national security).

189. *See* EYAL ZAMIR & BARAK MEDINA, LAW, ECONOMICS, AND MORALITY (forthcoming), *available at* http://ssrn.com/abstract=1438052 (defending the consistency of deontological rights and cost-benefit analysis in the counterterrorism setting). Furthermore, as Stephen Holmes and Cass Sunstein have demonstrated, all rights are ultimately associated with a price tag; without a financial commitment to enforcing certain rights—for example, by maintaining an effective court system and enforcement apparatus—rights lose their meaning. They argue that taxes are necessary for a state to protect its citizens because funding is necessary for security measures. STEPHEN HOLMES & CASS R. SUNSTEIN, THE COST OF RIGHTS: WHY LIBERTY DEPENDS ON TAXES 146 (1999) ("A government that enforces and protects rights, moreover, cannot do so unless it channels scarce tax revenues to public uses . . . . Property rights have costs because, to protect them, the government must hire police officers."). Thus, a purely deontological conception of rights in this area is ultimately of dubious

unconstrained by deontological limits may promote rights compliance more effectively than the present regime in a number of respects.

First, precisely because its scope is not limited by the present contours of First or Fourth Amendment doctrine, rationality review is well positioned to supply more wide-ranging protections against potentially overbearing intelligence programs. For example, a widespread human intelligence program might flunk cost-benefit review because the information sought is publicly available in academic literature and a costly invasion of privacy is therefore not justified. Such a claim would not be cognizable under current constitutional doctrine. Similarly, a data-mining program could run afoul of rationality review, even if current constitutional law furnishes no basis for enjoining the government from engaging in it. In other words, rationality review shows the way to an intelligence governance regime that could expand on the relatively paltry array of rights currently protected under constitutional law.

Rationality review would thus represent a practical alternative to the suggestion, made by a number of scholars, that constitutional doctrine should be revised to take aim at the pervasiveness of contemporary intelligence practice.[190] Some ground their objections to aspects of domestic intelligence in its capacity to chill speech and association.[191] Jed Rubenfeld rests his critique on an unorthodox account of the Fourth Amendment.[192] He disputes the familiar understanding (following Justice Harlan's concurrence in *Katz v. United States*[193]) that the Fourth Amendment is centrally concerned with protecting reasonable expectations

explanatory or practical value.

190. *See, e.g.*, United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313–14 (1972) ("National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. . . . [S]o also is there greater jeopardy to constitutionally protected speech. . . . The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'").

191. *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007) (arguing that the First Amendment must figure in surveillance law); Strandburg, *supra* note 55, at 747 ("The potential chilling effect due to relational surveillance poses serious risks not only to individual privacy, but to the First Amendment rights to freedom of association and assembly.").

192. Jed Rubenfeld points out that unlike the amendments that follow it, which speak in terms of protecting the individual ("person" or "accused") against the coercive power of the criminal justice system, the Fourth Amendment speaks in terms of protecting the security of "the people." Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 119–22, 130–32 (2008). He goes on to observe that "each individual's capacity to have a personal life depends in part on others' having that capacity as well—which is perhaps the decisive reason why the Fourth Amendment's right-holder is collective, rather than singular." *Id.* at 130–31.

193. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

of privacy.[194] Instead, he contends that the Fourth Amendment ought to be read as protecting against a kind of general insecurity that may affect "the people" as a whole. To Rubenfeld, domestic intelligence threatens to promote a kind of insecurity that he defines as "the stifling apprehension and oppression that people would justifiably experience if forced to live their personal lives in fear of appearing 'suspicious' in the eyes of the state."[195]

These critiques are powerful and capture something important about the new risk assessment paradigm of domestic intelligence. Indeed, it is with precisely the sorts of concerns raised by these scholars (and, more concretely, the historical experience of rampant abuses within the intelligence arena) in mind that I offer my account of what a robust governance regime rooted in rationality review ought to look like. As Benjamin Wittes contends, "Making . . . accountability mechanisms more pervasive, vibrant, regular, rigorous, and—to the extent possible—public offers a better avenue for restraining executive abuse than pretending to subject acquisition of data to judicial review that isn't real."[196]

Second, the rationality review I advocate could (and should) be wielded to review a wider range of intelligence programs from a larger set of institutions than are currently subject to federal governance. In particular, state and local intelligence regimes, which have grown in scale and prominence in recent years, would be part of a centralized review process. For example, rationality review could be employed to reject a proposed state-led initiative to gather certain kinds of intelligence on the grounds that the FBI was already engaged in the sort of intelligence analysis under discussion and that duplicating the national-level effort could not be justified in view of the costs of the proposed program. Increasing the number of agencies practicing domestic intelligence that are subject to a governance regime represents an important gain for overall

194. Rubenfeld, *supra* note 192, at 105–15.

195. *Id*. at 127.

196. WITTES, *supra* note 127, at 253. Wittes's judgment may be too harsh. *See infra* Part IV.B. There is a role for robust judicial review of domestic intelligence. *See also* Rachel E. Barkow, *Separation of Powers and the Criminal Law*, 58 STAN. L. REV. 989 (2006) (arguing for the application of separation of powers in criminal law to the same extent as in administrative law and that a significant advantage of administrative law over criminal law lies in its ability to address structural abuses at the appropriate level of generality). *Cf.* TERRORISM, GOVERNMENT, AND LAW: NATIONAL AUTHORITY AND LOCAL AUTONOMY IN THE WAR ON TERROR (Susan N. Herman & Paul Finkelman eds., 2008) (suggesting that an opportunistic embrace of federalism by certain liberal cities and states might offer the strongest structural protections against an aggressive national government).

rights protection.[197]

Third, and perhaps most significantly, rationality review protects rights more effectively than the current regime by being more attuned to questions of efficiency. Important intelligence gains do not necessarily flow from the most ambitious or far-reaching programs. Indeed, as critics of data mining have argued, for example, casting the widest possible intelligence net is frequently misguided from the standpoint of generating useful intelligence.[198] Indiscriminate human intelligence operations are similarly likely to yield relatively little useful intelligence.[199] In addition to being ineffective, these broad-gauged intelligence programs tend to correlate with being highly invasive of rights: the less precision built into the intelligence program, the more likely it is to acquire information about individuals removed from any threat, which, in turn, unhelpfully occupies the time of more intelligence professionals. Thus, as what might be described as an ancillary benefit, rationality review affords substantial rights protections by being attuned to the need for more focused intelligence programs. In the language of a leading European student of intelligence governance, oversight of "efficiency" and "propriety" are inherently complimentary and are not two unrelated categories.[200]

---

197. Cynthia Henry, *EPA Audit Finds DEP Flawed*, PHILA. INQUIRER, Aug. 28, 2009, at B1 (discussing how a recent audit of the New Jersey state environmental agency by the federal EPA uncovered the need for substantial improvements). Of course, local and state participation in federal intelligence oversight must be sufficiently voluntary to pass muster under the standard set out in *Printz v. United States*, 521 U.S. 898 (1997).

198. *See* PROTECTING INDIVIDUAL PRIVACY, *supra* note 56, at 24 (drawing attention to the absence of proof of the effectiveness of many data-mining programs).

199. They may also promote more "blowback" measures, for example, in community distrust of the government that impedes the ability of intelligence agencies to obtain vital information from the public. *See* SCHULHOFER, *supra* note 37, at 66 (describing the naïve "the more intelligence the better" view, which promotes compiling intelligence "as if we had repealed the law of diminishing marginal returns").

200. *See* Marina Caparini, *Controlling and Overseeing Intelligence Services in Democratic States*, *in* DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES: CONTAINING ROGUE ELEPHANTS 3, 8–9 (Hans Born & Marina Caparini eds., 2007). Furthermore, administrative bodies focused exclusively on issues of civil liberties may tend to become marginalized, especially within the intelligence community. The curious fate of the president's Privacy and Civil Liberties Board is a case in point. *See* Christopher Flavelle, *Disappearance of Privacy Board from White House Web Site Raises Questions*, PROPUBLICA, July 14, 2009, http://www.propublica.org/ion/changetracker/item/disappearance-of-privacy-board-from-whitehouse-website-raises-questions-714. *See also* Eli Lake, *Liberties Oversight Panel Gets Short Shrift*, WASH. TIMES, Feb. 2, 2010, at A1 (discussing the criticism against President Obama for not filling positions on the Privacy and Civil Liberties Oversight Board, especially in light of the Christmas Day attack).

3. Coordinated Intelligence

Not only does rationality review pave the way for more accurate and more rights-protective intelligence, it also lays the methodological foundation for a more coordinated and consistent intelligence process, and one with more robust and centralized accountability mechanisms. "Information sharing"—or its absence—has been one of the key motifs in discussions of intelligence after 9/11. The problem may arise because of bureaucratic infighting or because the right mechanisms (technological and administrative) do not exist to pool intelligence. Rationality review takes aim at both. It reduces the risk of egregious husbanding of intelligence within agencies by forcing information about proposed intelligence programs into the (relative) open. It inevitably also leads to more dialogue between agencies by creating a "common language" spoken by all elements of the intelligence community regardless of their particular specialties or mandates.

This common language, in turn, furnishes the starting point for a reviewing body (patterned on OIRA) to "check the agency's work" in the sense of reviewing underlying calculations (as appropriate), while also noting where whole categories of costs and benefits have been ignored.[201] The record generated by rationality review is of potentially more widespread use. It may also be employed by intelligence managers and strategists trying to understand the long-term consequences of a program or to refine the way that intelligence is practiced and governed.

B. JUDICIAL REVIEW FOR COMPLIANCE

Central to American administrative law and practice is judicial review of agency action: the idea that decisions taken by agencies are subject to oversight by the courts. Agency actions are subject to review on a number of bases.[202] Parties may challenge the constitutionality of an agency action—for example, on the ground that it violates the separation of powers or the nondelegation doctrine or the right of free speech. They may raise an objection rooted in the agency's interpretation of law, causing the court to consider application of so-called *Chevron* deference.[203] Alternatively, they

201. *See infra* Part IV.B. Rationality review also paves the way for meaningful judicial review of agency action for compliance with its own mandate.

202. *See* 5 U.S.C. § 706 (2006) (authorizing a reviewing court to "decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action").

203. Following *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984), courts defer to an agency's statutory interpretation of its organic statute in cases where

may seek to overturn an agency decision by asserting a defect in the agency's process. The court may also entertain a challenge based on a different sort of claim: that in view of the agency's stated (and putatively legitimate) ends, the means it selected for regulating were misguided. Whether setting aside the agency action as "arbitrary and capricious"[204] or as failing to withstand a judicial "hard look,"[205] the court has the power to police the ways in which the agency complies with its own stated regulatory agenda.

To the extent that judicial review has figured in the governance of intelligence, it has been in the loose sense that judges have figured in some aspects of intelligence oversight. For example, Article III judges who sit on the FISC play an important role in the review of applications for electronic surveillance for compliance with the statute's requirements (as well as with bedrock constitutional guaranties). As discussed above, however, this role is highly circumscribed, as in the case of the issuance of search warrants. Once the FISC judge has given assent to a government surveillance application, the judge's job as an intelligence overseer is basically done. Typically, there is no opportunity to test the constitutionality of the intelligence at trial as there is (at least in concept) in criminal law. More generally, courts may entertain civil suits alleging violations of rights stemming from intelligence programs. As discussed above, suits of this sort immediately run into a number of practical and doctrinal obstacles.[206]

The regulatory model of intelligence governance implies a different

---

Congress was silent or ambiguous in drafting the text and where the agency's interpretation is a "permissible construction." Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842–43 (1984).

204. 5 U.S.C. § 706(2)(A). *See, e.g.*, Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 40–44, 57 (1983) (holding, in a case in which an agency rescinded a regulation, that under arbitrary and capricious review a court could strike down agency action that was not supported by a "reasoned analysis," which requires that agencies more thoroughly consider relevant facts and alternatives); Citizens to Preserve Overton Park, Inc. v. Volpe, 401 U.S. 402, 416 (1971) (holding that arbitrary and capricious review requires courts to examine whether an agency decision was "based on a consideration of the relevant factors and whether there has been a clear error of judgment" (citations omitted)), *overruled on other grounds by* Califano v. Sanders, 430 U.S. 99 (1977). *See generally* SEC v. Chenery Corp., 318 U.S. 80 (1943) (requiring agencies to provide and conform to ex ante rationales for their actions).

205. Greater Boston Television Corp. v. FCC, 444 F.2d 841, 851 (D.C. Cir. 1970) ("Assuming consistency with law and the legislative mandate, the agency has latitude not merely to find facts and make judgments, but also to select the policies deemed in the public interest. The function of the court is to assure that the agency has given reasoned consideration to all the material facts and issues. This calls for insistence that the agency articulate with reasonable clarity its reasons for decision, and identify the significance of the crucial facts, a course that tends to assure that the agency's policies effectuate general standards, applied without unreasonable discrimination." (footnotes omitted)).

206. *See supra* Part II.

way to conceptualize judicial review of intelligence in a manner that resonates with the experience of courts in administrative law. At some regular interval after an agency has implemented a particular intelligence program (following successful rationality review), a court should review the agency's program for fidelity to the agency's own stated (and previously approved) objectives. In focusing on how the agency has implemented the intelligence program in practice, a court could determine whether, in view of empirical evidence, the actual costs and benefits of the program are roughly in line with those that were anticipated prior to the program's implementation. Even more basically, the court could determine whether the agency was remaining true to the stated goals and limitations of the program's mandate.

In reviewing compliance with the program's mandate, the court would take aim at one of the core problems with intelligence (and one of the core liabilities of the current regime of intelligence governance): intelligence drift. By "intelligence drift," I mean to refer to two subtly different but interrelated phenomena. The first is the tendency of an intelligence program to begin by focusing on assessing risk A and later to morph insidiously into a program focusing on a totally different risk B. While drift of this sort may be justified on some occasions as an appropriate response to an evolving risk (or, at any rate, an evolving understanding of a constant risk), it is just as likely to come about because the intelligence officials running a program suffer from the bureaucratic equivalent of a wandering eye. The second type of drift implicates the extreme reluctance with which intelligence agencies acknowledge that a program has outlived its utility.[207] The tendency for intelligence agencies to want to keep drilling in dry wells is precisely what has led to abusive and ineffective intelligence in the past.

Judicial review of this sort would play an important role in the overall governance of domestic intelligence. In addition to having to justify prospective intelligence programs for cost-benefit rationality ex ante, intelligence agencies would be required to stand by their initial plans (or put forth compelling justifications for any departure from them) ex post. Furthermore, Article III judges are well positioned to engage in this sort of judicial review. Because the scope of the review is limited to the agency's compliance with its original plan (concerning which there will have been a developed record stemming from rationality review), the court need not

207. As the sustained and costly search for weapons of mass destruction in Iraq long after the initial invasion amply demonstrates, it can be difficult for intelligence agencies to acknowledge that a collection effort has proved fruitless.

develop expertise in the utility of one or another form of intelligence gathering. No different from the D.C. Circuit sitting in review of agency action across the regulatory state,[208] the reviewing court would simply be looking for the agency's compliance with its own carefully delineated plan.[209]

C. PLURALISM

Ever since the high watermark of good government activism in the late 1960s and 1970s, "the basic principle that the 'public' ought to play a role in regulatory decisions involving health and environmental risks has not been seriously questioned."[210] While Peter Gill is no doubt correct when he observes of the history of popular involvement in intelligence matters that "the 'polyarchical' processes of organised group politics do not penetrate very often into the secret state and do not constitute democratic control over intelligence policy,"[211] regulatory governance of domestic intelligence should entail greater reliance on pluralistic processes.[212]

Pluralism in the form of consulting interested parties can play numerous important roles in the intelligence arena. First, it can help shape the normative framework for determining the proper scope of an inevitably contested process like domestic intelligence as risk assessment. As John

208. *See* Jack Goldsmith, *Long-Term Terrorist Detention and Our National Security Court* 6–8 (Brookings Inst. Counterterrorism and Am. Statutory Law Series, Paper No. 5, 2009), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2009/0209_detention_goldsmith/0209_detention_goldsmith.pdf. (adumbrating a model system that identifies a class of individuals that would be subject to detention as enemy combatants while allowing for judicial review). One significant difference is the absence of an adversarial lawsuit triggering the judicial review I defend. Some regard this as a potentially significant constitutional defect. *See, e.g.*, Posner, *supra* note 105, at 255 (noting that as an Article III court, the FISC may not render advisory opinions). The best counterargument is probably that the review process ought to be regarded from the standpoint of constitutional law as the equivalent to reconsideration by the court of a search warrant.

209. This is not to deny that there will be cases that will require reviewing judges to make determinations about the nature of the intelligence process. Even using the system I have set out, some involvement in intelligence is inevitable. Where my proposal marks a break with current practice, however, is in relieving judges of the need to decide the overall value of a given intelligence program and in injecting robust, ongoing judicial involvement in intelligence governance.

210. Thomas O. McGarity, *Public Participation in Risk Regulation*, 1 RISK 103, 103 (1990).

211. GILL, *supra* note 70, at 303. *See generally* Thomas C. Beierle & Jerry Cayford, *Environmental Decision Making: What Does Public Participation Add?*, ADMIN. & REG. L. NEWS, Winter 2003, at 6 (summarizing the conclusions of their book, THOMAS C. BEIERLE & JERRY CAYFORD, DEMOCRACY IN PRACTICE: PUBLIC PARTICIPATION IN ENVIRONMENTAL DECISIONS (2002)).

212. *See, e.g.*, Pildes & Sunstein, *supra* note 158, at 86–89 (criticizing Justice Breyer's technocratic theory of administration for failing to sufficiently accommodate public values and perceptions of risk). *See also* WILLIS, *supra* note 167, at 5 (explaining that "[r]isk is a social construct that incorporates value judgments about context and cause").

Graham notes, "The important role of values in risk analysis is not an argument against risk analysis."[213] Interest group contestation in this area can be an important tool for allowing multiple viewpoints to be aired and normative judgments to be appropriately calibrated. This is especially true in view of the prevalence and salience of various heuristic biases in the area of counterterrorism more broadly.[214]

Second, pluralism in the form of input from the community of subject matter experts can help improve the scientific integrity—and hence, the ultimate utility—of intelligence.[215] While members of the intelligence community must shoulder the ultimate responsibility for "getting it right," a process akin to "peer review" may prove beneficial.[216] In his ethnography of intelligence analysts, Rob Johnston observes that analytic blunders are in some ways dependent on the culture of secrecy that prevails inside the intelligence community.[217] Richard Posner and Luis Garciano further develop this observation by noting that intelligence analysis is prone to mistakes because of, inter alia, the organizational pathologies of "groupthink" and "information cascades."[218] Ideally, under conditions of greater participation by outside experts, domestic intelligence can avoid

213. John D. Graham, *The Risk Not Reduced*, 3 N.Y.U. ENVTL. L. J. 382, 400 (1995).

214. *See* Sunstein, *supra* note 181, at 121–22 (discussing how emotional concerns and fears regarding terrorism cloud the ability of individuals to effectively evaluate threats, which results in widespread, unjustified public fear); Tversky & Kahnenman, *supra* note 182 (reviewing studies of the "availability" heuristic and how it shapes individuals' assessments of frequency). For the view that some of these popular attitudes toward counterterrorism ought to be taken into account by a risk regulatory system, see Pildes & Sunstein, *supra* note 158, at 48–64 (arguing that some lay perspectives represent a different system of values rather than cognitive error). *But see* W. Kip Viscusi, *Risk Equity*, *in* COST-BENEFIT ANALYSIS, *supra* note 162, at 7, 31 (arguing that "[t]he objective of government policy . . . should be to reduce objective risks to populations and to generate actual improvements in health rather than . . . illusory increases in well-being" and thus that risk assessment should not be concerned with the risks "people perceive that they face").

215. The heightened role for outside experts in the intelligence process is related, in general terms, to the growth of open-source intelligence ("OSINT"). OSINT is predicated on the idea that much of what there is to know about a subject is available in academic literature and reportage and does not require resort to clandestine collection or original analysis. Concerning OSINT, the greatest challenge is typically how to exploit information to useful effect without becoming overwhelmed by the quantity of data available through open sources. *See, e.g.*, Stephen Mercado, *A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age*, *in* SECRET INTELLIGENCE: A READER 78 (Christopher Andrew, Richard J. Aldrich & Wesley K. Wark eds., 2009).

216. Congressman Frank Wolf has recommended instituting a "red team" or "Team B" approach to counterterrorism intelligence analysis whereby outside experts would offer a perspective potentially challenging the received wisdom within the government. *See* Bruce Hoffman, *American Jihad*, NAT'L INT., Apr. 20, 2010, http://www.nationalinterest.org/Article.aspx?id=23200.

217. JOHNSTON, *supra* note 148, at 11–13.

218. Luis Garcano & Richard A. Posner, *Intelligence Failures: An Organizational Economics Perspective*, J. ECON. PERSP., Fall 2005, at 151, 153–55.

regulatory "ruts" owing to processes "that track[] developments in emerging science or technology."[219] As Andrew Goldsmith has argued, "The limits of existing expertise in [the area of counterterrorism] . . . support the case for . . . drawing upon a wider range of inputs from the public."[220]

Third, pluralism would afford communities disproportionately affected by domestic intelligence the opportunity to share their particular concerns with the government. As former senior FBI official Michael Rolince has observed, although

> there is concern that [the new guidelines] may encourage the violation of U.S. civil rights through the harassment of innocent persons, particularly in Muslim and Arab communities . . . [t]he new guidelines may place FBI agents in greater contact with Arab Americans and other ethnic minority groups; this would, indeed, be a positive outcome.[221]

Outreach of this sort is vital not only because of the profound civil rights issues at stake, but also because outreach ensures the ongoing willingness of members of these communities to provide the vital information they possess to security officials.[222]

---

219. *See* Lynn E. Blais & Wendy E. Wagner, *Emerging Science, Adaptive Regulation, and the Problem of Rulemaking Ruts*, 86 TEX. L. REV. 1701, 1735 (2008) (suggesting a regulatory system based on "revision rulemaking" by encouraging technological innovation while creating a flexible evaluation system). *Cf.* Art Brown, Op-Ed, *Intelligence Boosters*, N.Y. TIMES, Dec. 14, 2008, at WK11 ("[The CIA] does not sufficiently tap into the expertise that exists across the breadth of America. The human spy components of the C.I.A. live in a cocoon of secrecy that breeds distrust of outsiders. This is one reason very few officers have BlackBerrys, and those few who do usually leave them in their cars when they go to work. Despite their reputation as plugged-in experts on other countries, many C.I.A. officers do not even have Internet access at their desks. Worse yet, they don't think they need it.").

220. Andrew Goldsmith, *The Governance of Terror: Precautionary Logic and Counterterrorist Law Reform After September 11*, 30 LAW & POL'Y 141, 163 (2008). Goldsmith goes on to call for "an *institutionalization of pluralism*, whereby different assessments of 'the problem' as well as 'what should be done' can be more openly investigated and discussed." *Id.*

221. Rolince, *supra* note 88. One well-documented problem concerns the barriers to entry into the intelligence community of individuals with particularly useful linguistic and cultural skills due to agency hiring practices. As the former Director of National Intelligence Michael McConnell put it,

> The responsibility to protect sources and intelligence-collection methods from unauthorized disclosure has heightened some organizations' risk aversion. As a result, intelligence agencies have faced significant obstacles in hiring some of the people they need most: first- and second-generation Americans with fluency in languages ranging from Albanian to Urdu and with unique political, technical, or scientific skills. These men and women possess cultural insights and skills that no amount of teaching can impart. If the intelligence community is going to reach out to native speakers, it must change its recruitment practices, which currently make it difficult to hire such candidates.

Mike McConnell, *Overhauling Intelligence*, FOREIGN AFF., July/Aug. 2007, at 49, 56.

222. As "repeat players" within their respective communities, local police may be more attentive to their distinctive needs than federal agents. *See generally* Susan N. Herman, *Collapsing Spheres: Joint Terrorism Task Forces, Federalism, and the War on Terror*, *in* TERRORISM, GOVERNMENT, AND LAW, *supra* note 196, at 78. For a critical assessment of the scholarly tendency to praise the role of local

D. TRANSPARENCY

Related to—and underwriting the possibility of—pluralism in domestic intelligence governance is the concept of transparency. At first blush, transparency seems like an odd fit with an intelligence community that inevitably carries out much of its work in secret; but as Director of National Intelligence Dennis Blair testified at his confirmation hearing, "There is a need for transparency and accountability in a mission where most work necessarily remains hidden from public view."[223] Blair further testified that he intends to "communicate frequently and candidly with the oversight committees, and as much as possible with the American people."[224]

One respect in which the domestic intelligence state can move in the direction of greater transparency is in the disclosure of the nature and scope of the legal authority it exercises. The very fact that the current *Attorney General's Guidelines* covering domestic intelligence (as well as the recently revised executive order governing foreign and domestic intelligence[225]) are published (almost in their entirety) and are available on the Internet represents a break from past tradition.[226] Another sense in which the domestic intelligence apparatus could achieve greater transparency is in the continued publication of its analytic findings where senior intelligence officials offer insights into the major threats of the day and nonclassified versions of National Intelligence Estimates are made public.[227] For example, Blair recently testified that the "primary near-term

authorities in counterterrorism, see Samuel J. Rascoff, *The Law of Homegrown (Counter)Terrorism*, 88 TEX. L. REV. (forthcoming 2010).

223. Scott Shane, *Blair Pledges New Approach to Counterterrorism*, N.Y. TIMES, Jan. 23, 2009, http://www.nytimes.com/2009/01/23/us/politics/23blaircnd.html?scp=1&sq=&st=nyt.

224. *Id.*

225. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), *reprinted as amended in* 50 U.S.C.S. § 401 (LexisNexis 2009) (organizing and delineating certain authorities of the intelligence community). Executive Order 12,333 was amended by Executive Order 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

226. *See, e.g.*, Martin C. Libicki & David R. Howell, *Privacy and Civil Liberties Protections in a New Domestic Intelligence Agency*, *in* THE CHALLENGE OF DOMESTIC INTELLIGENCE, *supra* note 39, at 149, 167–69 (discussing the pros and cons of adopting policy of revealing to individuals the information that a domestic intelligence agency has about them).

227. Historically, the government has resisted revealing specific intelligence data through, for example, the FOIA process on the ground that partial revelations might ultimately reveal the larger strategic purpose behind the intelligence. *See, e.g.*, David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 633–45 (2005) (discussing the government's national security claims in opposition to FOIA requests before 9/11). The upshot of my account is that the government theory has it exactly backwards. Whereas the revelation of specific details may be dangerous or otherwise unacceptable, the disclosure of the "big picture" will frequently

security concern of the United States is the global economic crisis and its geopolitical implications."[228] The point would be for the domestic intelligence apparatus to more candidly describe the nature and the intensity of the threat, past the superficial and frequently misleading color-coded alerts of the sort issued for the last six years by the DHS.[229] A good example is supplied by the MI5's website, which contains thoughtful, detailed information about the terrorist threat to the United Kingdom, as well as the government's policy for countering it.[230]

Disclosures of this sort do, to be sure, entail certain risks. For example, politicians may be inclined to exaggerate a threat that has been reported by the intelligence agency for narrow political gain, or to minimize an intelligence-driven analysis that undercuts a preferred political platform. Citizens (who will typically lack a context for understanding the threat baseline) may fail to understand the nature of the assessment and may tend to overreact to it. To the extent that the threat tracks defined religious or ethnic groups, certain civil liberty concerns might be implicated. Additionally, the intelligence apparatus itself may take advantage of opportunities to disclose information in order to promote the agency's own perceived self-interest, or perhaps even to engage in disinformation. In general, a more robust regime of regulatory governance of domestic intelligence requires greater emphasis on peeling back layers of secrecy.

V. THE INSTITUTIONAL LIFE OF REGULATORY GOVERNANCE

I have argued that domestic intelligence governance ought to draw on some of the most fundamental features and concepts of administrative law,

---

be harmless to the government's interest.

228. *See* Posting to CNN Wire, http://cnnwire.blogs.cnn.com/2009/02/12/economy-is-security-threat-dni-says/ (Feb. 12, 2009, 16:52 EST).

229. This much-maligned system has recently been reviewed by a panel of experts. *See* HOMELAND SEC. ADVISORY COUNCIL, U.S. DEP'T OF HOMELAND SEC., HOMELAND SECURITY ADVISORY SYSTEM TASK FORCE REPORT AND RECOMMENDATIONS (2009), http://www.dhs.gov/xlibrary/assets/hsac_final_report_09_15_09.pdf. Half of the review panel said the alerts should be scrapped, half said they should be retained. *Id.* at 2. If retained, the entire review panel agreed that the color alerts should be reformed, with more rigor applied to raising the threat level (and a process to automatically lower it in the absence of an identified persisting threat) as well as more specific and detailed information given to the public when the threat level is altered (including actions to be taken to counter the threat). *See id.* at 2–3. These reforms are to be undertaken to provide transparency and thereby renew public confidence and lessen the danger of politicization of the alert system. *See id.*

230. MI5 Security Service, Threat Levels, http://www.mi5.gov.uk/output/threat-levels.html (last visited Mar. 1, 2010).

including rationality review, judicial review of agency action, and pluralism. If a regulatory approach to intelligence governance is to succeed, however, these ideas must be instantiated in a set of concrete institutions and practices. Rationality review must be implemented by an agency with the right mixture of expertise and objectivity; judicial review must have teeth but also sensitivity to context; and pluralist processes must be allowed to develop within a habitually secretive intelligence apparatus. In this part, I provide a framework for how regulatory governance can be achieved in practice. My starting point is a set of developments in intelligence governance over the last few years that make the possibility of achieving regulatory governance that much more real. These developments—including the creation of the Office of the Director of National Intelligence ("ODNI"), the substantial overhaul of the FISA statute, and the suggestion (faint though it currently is) of new avenues for interest group participation in intelligence matters—have not been appreciated for what they are: part of a nascent regulatory turn in domestic intelligence governance.

A. ODNI: RATIONALITY REVIEW

Created in 2004 by the Intelligence Reform and Terrorism Prevention Act ("IRTPA"), the ODNI is perched atop the sixteen agencies that make up the loosely knit intelligence community. With a staff of around 1500,[231] the ODNI was designed in large part to coordinate the efforts of these various organizations, encourage the flow of information between and among them, and synthesize intelligence for the president.[232] Predictably, the ODNI has had trouble getting off the ground and establishing its superagency status.[233] Even before the ink on the intelligence law was dry, the ODNI had been stripped of a good deal of the budgeting authority[234]

231. *See* O'Connell, *supra* note 36, at 1667–68 (discussing the creation and development of the Director of National Intelligence's powers as a result of the IRTPA). This number is an estimate—and the Director of National Intelligence may actually be hiding the actual size of its staff. *See* Posting of Jeff Stein to SpyTalk, http://blogs.cqpolitics.com/spytalk/2009/07/spy-agencies-hiding-true-numbe.html (July 22, 2009, 21:55 EST).

232. *See* RICHARD A. BEST, JR., CONG. RESEARCH SERV., REPORT NO. RS21948, THE NATIONAL INTELLIGENCE DIRECTOR AND INTELLIGENCE ANALYSIS (2004) (discussing the creation of the ODNI and its role in the intelligence gathering process). *See also* McConnnell, *supra* note 221, at 50–54.

233. For a sense of the early predictions of doom, see Philip Shenon, *Critics Say Bush's Intelligence Chief Would Be Toothless*, N.Y. TIMES, Aug. 4, 2004, at A12. For a sense of the more current troubles, see *A Bad Job: Restructuring Intelligence*, ECONOMIST, Jan. 13, 2007, at 39.

234. *See* Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 102A(c), 118 Stat. 3638, 3644–55 (detailing the budgetary powers that would be vested in the Director of National Intelligence ("DNI"), including the ability to determine the most efficient and effective way to allocate ODNI funds); 150 CONG. REC. S11,946–47 (daily ed. Dec. 8, 2004) (statement of Sen. Specter). For a sense of the politics behind this stripping of budgetary authority, see Gail R.

that had been contemplated in response to the 9/11 Commission's complaint that the CIA director had historically faced the impossible task of "direct[ing] agencies without controlling them . . . [or] control[ling] their purse strings."[235] The fierce independence of the agencies, most notably of the CIA, has made intelligence community integration exceedingly difficult,[236] and without having succeeded at that defining role, the ODNI has found itself grasping for a purpose.[237] All the while, the head of the ODNI, the Director of National Intelligence ("DNI"), has found himself in the position of serving in the time-consuming role as the president's personal intelligence briefer.[238] To a large degree, the ODNI remains, in the words of former CIA deputy director of operations Jack Devine, "an unnecessary bureaucratic contraption with an amazingly large staff."[239] Put simply, today's ODNI is an institution searching for a mission.[240]

Chaddock, *Where Do Reforms Urged by 9/11 Commission Stand?*, CHRISTIAN SCI. MONITOR, July 22, 2009, http://www.csmonitor.com/USA/Politics/2009/0722/where-do-reforms-urged-by-911-commission-stand.

235. 9/11 COMMISSION REPORT, *supra* note 41, at 357.

236. *See* Mark Mazzetti, *Turf Battles on Intelligence Pose Test for Spy Chiefs*, N.Y.TIMES, June 8, 2009, http://www.nytimes.com/2009/06/09/us/politics/09intel.html?_r=1 (discussing the dispute between the CIA and the DNI over which agency would be authorized to manage American intelligence personnel overseas).

237. *See* Pamela Hess, *CIA, Intel Director Locked in Turf Battle*, ASSOCIATED PRESS, May 27, 2009; David Ignatius, Editorial, *Duel of the Spy Chiefs: A Turf War Exposes a Botched Reorganization*, WASH. POST, June 11, 2009, at A23 (explaining that the battle over appointing overseas agents stemmed from overlapping powers—those given to the DNI in the IRTPA and those that have been vested in the CIA since the Cold War).

238. Arthur Hulnick, a former CIA officer who used to edit the President's Daily Brief, reports that DNI John Negroponte would spend up to 60 percent of his time preparing for and conducting the Daily Brief, requiring an entire staff to aid this process. *See* Arthur S. Hulnick, *Intelligence Reform 2008: Where to From Here?*, 21 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 621, 624 (2008) (explaining that there had not been significant reforms in the intelligence community but that the new administration had plans for reforming and updating the system, although it is questionable whether the plans will be successful due to bureaucratic inertia). Similarly, the ODNI Inspector General recently concluded that the DNI has had to devote much of his time to providing intelligence support to the President and senior policymakers. EDWARD MAGUIRE, ODNI, OFFICE OF INSPECTOR GEN., (U) CRITICAL INTELLIGENCE COMMUNITY MANAGEMENT CHALLENGES 2 (2008), *available at* http://www.fas.org/irp/news/2009/04/odni-ig-1108.pdf; Mark Mazzetti, *Report Faults Spy Chief for Inaction on Turf Wars*, N.Y. TIMES, Apr. 2, 2009, at A15 (reporting that "the inspector general[] said . . . it might be wise for the intelligence chief to limit the number of days he delivers the president's daily brief in the Oval Office").

239. Jack Devine, Editorial, *An Intelligence Reform Reality Check*, WASH. POST, Feb. 18, 2008, at A17. As former counterterrorism official Richard Clarke explained, with the way the ODNI currently functions, "You're left with the impression that it wouldn't make any difference if they didn't exist." *See* Lawrence Wright, *The Spymaster*, NEW YORKER, Jan. 21, 2008, at 42. Rush Holt, a member of the House Intelligence Committee, recently observed that "[t]he D.N.I. seems to have no authority to manage and coordinate the agency he is supposed to coordinate." *See* Mazzetti, *supra* note 238.

240. Faced with an ambiguous mission, the ODNI has pursued certain seemingly quixotic goals, sometimes to the intense displeasure of other members of the intelligence community. In one closely

Faced with the daunting challenge of carving out a meaningful institutional niche, the ODNI ought to embrace the mission of regulatory governance of intelligence. First, the ODNI's authorizing statute and legal authorities make the office (or some part of it to which the DNI assigns the task) uniquely well positioned to consider the costs and benefits of proposed intelligence programs. Second, the office possesses the requisite mix of expertise and detachment to make informed but dispassionate decisions about intelligence programs. Third, embracing the role of regulatory governance would contribute meaningfully to the furtherance of the ODNI's twin goals of facilitating information sharing across the intelligence community and providing overarching strategic management of American intelligence. In sum, the ODNI—or some office within it—ought to aspire to play the role for the intelligence community that OIRA has played for the administrative state beginning with Reagan's Executive Order 12,866.[241]

The ODNI has the legal mandate to employ rationality review as part of domestic intelligence governance. While the ODNI's organic statute, the IRTPA, has been criticized for failing to provide specific guidance as to how the DNI ought to go about day-to-day tasks,[242] the statute's outline of the DNI's strategic objectives is fairly clear. First, the DNI is authorized to "direct[] the allotment or allocation of . . . appropriations."[243] Second, the DNI is empowered to function as the strategic manager of all intelligence; specifically, the DNI is to "establish objectives, priorities, and guidance for

watched case, the ODNI lost its bureaucratic battle. *See* Mark Mazzetti, *White House Sides with C.I.A. in Turf Battle*, N.Y. TIMES, Nov. 12, 2009, http://www.nytimes.com/2009/11/13/us/politics/13intel.html (noting that the White House "sided" with the CIA and upheld its longstanding prerogative of naming the top American intelligence official posted to each foreign country in the face of a challenge to that authority by the ODNI). Lingering tensions from that episode and others appear to have contributed to President Obama's recent decision to ask for Director Blair's resignation. *See* Mark Mazzetti, *Facing a Rift, U.S. Spy Chief to Step Down*, N.Y. TIMES, May 20, 2010, at A1.

241. The vision Justice Breyer outlined for newly created administrative groups may be applied to the ODNI as well:

> [T]he group must have a . . . risk-related *mission* . . . of building an improved, coherent risk-regulating system, adaptable for use in several . . . risk-related programs; the mission of helping to create priorities within as well as among programs; and the mission of comparing programs to determine how better to allocate resources to reduce risks.

See BREYER, *supra* note 178, at 60.

242. Commenting on one important aspect of oversight, intelligence veteran Robert Vickers pointed out that IRTPA "authorized the new DNI to 'ensure the elimination of waste and unnecessary duplication'" but "gave no specific guidance on how this should be done." Robert D. Vickers, Jr., *The Intelligence Reform Quandary*, 19 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 356, 357 (2006) (quoting Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 102A(f)(5), 118 Stat. 3638, 3649). *See also* 150 CONG. REC. S11,946–47 (daily ed. Dec. 8, 2004) (statement of Sen. Specter).

243. IRTPA § 102A(c)(5)(A), 118 Stat. at 3645.

the intelligence community,"[244] "determine requirements and priorities for . . . [the] collection, analysis, production, and dissemination of national intelligence,"[245] and "ensure the elimination of waste and unnecessary duplication"[246] among elements of the intelligence community. Third, the DNI presides over a Privacy and Civil Liberties Oversight Board[247] that oversees "regulations, . . . policies, and procedures" in order to "ensure that privacy and civil liberties are protected."[248] Taken together, these sources of authority—control over purse strings, a mandate to oversee intelligence programs and to prevent waste, and the requirement to protect civil liberties—track the basic functions of an agency conducting rationality review of intelligence programs.

Not only does the DNI have the necessary statutory power to engage in rationality review, but the DNI's office also possesses the core competences to discharge that role effectively. First, the DNI's office (which has a sufficiently large staff to tackle the daunting task of intelligence governance) possesses the requisite expertise in intelligence matters to provide meaningful governance. Steeped in the culture and technical capacities of intelligence, the ODNI is considerably more likely than congressional or judicial overseers to ask the right sorts of questions (without which governance approaches a rubber stamp). At the same time, the DNI enjoys sufficient distance from the various intelligence agencies that are subordinate to the ODNI to be relatively free from fear of agency capture. While the ODNI's initial employees generally came from the constituent intelligence agencies and may well have brought to their new jobs the professional biases of their former workplaces, increasingly, the ODNI staff is comprised of direct hires.

Finally, embracing the role of rationality review will not only strengthen intelligence governance, but it will also simultaneously help the

244. *Id.* § 102A(f)(1)(A)(i), 118 Stat. at 3648.

245. *Id.* § 102A(f)(1)(A)(ii), 118 Stat. at 3648.

246. *Id.* § 102A(f)(5), 118 Stat. at 3649.

247. *Id.* § 1061, 118 Stat. at 3684–88.

248. *Id.* § 1061(c)(2)(A), 118 Stat. at 3685. The Board itself has encountered some early turbulence related in part to claims of heavy-handed involvement by the White House. *See* Posting of Lanny Davis, *Why I Resigned from the President's Privacy and Civil Liberties Oversight Board—And Where We Go from Here*, HUFFINGTON POST, May 18, 2007, http://www.huffingtonpost.com/lanny-davis/why-i-resigned-from-the-p_b_48817.html (recalling informing fellow Board members of his decision to resign in a letter stating, "I also continue to be concerned that there may be current and developing anti-terrorist programs affecting civil liberties and privacy rights of which the Board has neither complete knowledge nor ready access," and referring to "substantial 'redline' edits submitted by the White House" (quoting Letter from Lanny Davis to Privacy & Civil Liberties Oversight Bd. Members (May 14, 2007))).

DNI realize the two most important strategic objectives of intelligence, both derived from the *9/11 Commission Report* (which supplied a conceptual roadmap for the ITRPA).[249] First, the DNI must facilitate information sharing—the lack of which, in the estimation of the 9/11 Commission, was a major contributing factor to the success of the attacks.[250] Above and beyond the ordinary flow of intelligence from the agencies to the DNI (for inclusion in the President's Daily Brief, for example), rationality review provides an important channel for generating information flows about intelligence programs from the agencies to the DNI.

In addition to being concerned about information flows, the framers of the intelligence reform law were clearly focused on the problem of the absence of overall leadership within the intelligence apparatus. Senator Joseph Lieberman quoted the testimony of Lee Hamilton, vice chairman of the 9/11 Commission:

> A critical theme that emerged throughout our inquiry was the difficulty of answering the question: Who's in charge? Who ensures that agencies pool resources, avoid duplication and plan jointly? Who oversees the massive integration and unity of effort to keep America safe? Too often the answer is no one.[251]

---

249. Multiple tributes to the 9/11 Commission's work in stimulating the creation of the ODNI appear in the CONGRESSIONAL RECORD, as politicians were eager to embrace the perceived political cover that the Commission, with its recently completed 9/11 COMMISSION REPORT, conferred. *See*, *e.g.*, 150 CONG. REC. S11,939 (daily ed. Dec. 8, 2004) (statement of Sen. Frist); *id*. at S11,940 (statement of Sen. Collins); *id.* at S11,941 (statement of Sen. Lieberman) (specifically noting that IRTPA implemented recommendations of the 9/11 COMMISSION REPORT); *id.* at S11,945 (statement of Sen. Specter). The White House similarly gave primary credit to the 9/11 Commission when it first announced plans to establish a new intelligence superagency. *See* Press Briefing by Andrew Card, White House Chief of Staff (Aug. 2, 2004), (transcript available at http://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040802-6.html). *See also* White House, Fact Sheet: Leading the Way on Reforming and Strengthening Intelligence Services (Sept. 8, 2004), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB144/20040908-5.html. Card also noted that the White House did get additional input from Judge Laurence Silberman of the D.C. Circuit and former Senator Chuck Robb, who were then in the process of conducting what would be known as the Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

250. For a compilation of the pieces of information that, if only shared across the intelligence community, would have prevented 9/11, see BOBBITT, *supra* note 131, at 307–08. For a short history of the fractiousness of the so-called intelligence community, see Wright, *supra* note 239. For a sense of the prominence information sharing achieved after 9/11, see COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S., REPORT TO THE PRESIDENT REGARDING WEAPONS OF MASS DESTRUCTION 320 (2005), *available at* http://govinfo.library.unt.edu/wmd/report/wmd_report.pdf ("No shortcoming of the Intelligence Community has received more attention . . . than the failure to share information.").

251. 150 CONG. REC. S11,942 (statement of Sen. Lieberman) (alteration omitted).

The intelligence reform statute, Lieberman went on to point out, "changes all of that," putting a single organization in charge of "overseeing the entire intelligence community and its multibillion-dollar budget."[252] Senator Arlen Specter was even more direct, noting that a fundamental objective of the DNI is to "manage the national intelligence program and oversee the agencies that contribute to it."[253] According to the second DNI director, Admiral Michael McConnell, the statute directs the DNI to "focus, guide, and coordinate" the intelligence community.[254] Once again, this objective would be greatly facilitated by the presence of regulatory review. While not taking the place of the other formal and informal mechanisms at the DNI's disposal for establishing leadership, the association of the DNI's office with intelligence governance enhances the DNI's claim to legitimate leadership of American intelligence.

B. FISA: JUDICIAL REVIEW OF INTELLIGENCE PROGRAMS

Another area in which there has been a recent change in the law, carrying potentially significant implications for regulatory governance of intelligence, is FISA. As discussed above, the statute historically provided that surveillance of Americans' telephone calls and emails for the purpose of obtaining "foreign intelligence information" be authorized by a specially convened Article III tribunal, the FISC. Traditionally, the FISC considered each application individually as a prerequisite for deciding the presence of authority in a process that essentially resembled (and was patterned on) the consideration by a federal court of a garden-variety wiretap application under Title III.

The rise of a risk-assessment model of domestic intelligence has brought about a fundamental addition to FISA practice.[255] Central to the FISA Amendments Act of 2008 is a provision that gives the FISC authority to issue what amounts to a "programmatic" or "basket" warrant for an entire intelligence program.[256] In order to conduct basket warrant–type

252. *Id*.

253. *Id.* at S11,947 (statement of Sen. Specter).

254. McConnell, *supra* note 221, at 50.

255. FISA has not changed its requirement for individualized court approval of surveillance applications as to "U.S. Persons" inside the United States. *See* Office of the Press Sec'y, U.S Dep't of Justice, Background Briefing by Senior Administration Officials on FISA 8 (Feb. 26, 2008) (transcript available at http://www.usdoj.gov/archive/ll/docs/background-briefing-fisa022608.pdf) ("We create a scheme that says, you do have to go to . . . court and get approval, just like you always have, if you want to target someone living in the United States—under traditional FISA.").

256. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438–48. *See also* Prieto, *supra* note 30, at 52–53 ("The new act does not require individual warrants from the FISA Court for each acquisition when the target is a non-U.S. person located outside the United States. In

surveillance in accord with the FISA Amendments Act, the government must seek an order of approval from the FISC,[257] which requires the submission to the FISC of attestations (signed by the Attorney General, as well as the DNI) of its compliance with statutory requirements, as well as of the details of procedures it has adopted in order to ensure such compliance.[258] If the government fails to convince the FISC that it satisfies the statutory requirements, the FISC can deny approval of a basket warrant, and the government may take an appeal to the FISA Court of Review.[259]

The issuance of programmatic warrants is in some respects analogous to the well-established practice of issuing administrative warrants in other areas, such as public health.[260] What is nevertheless surprising about the

such cases, the FISA Court no longer reviews each application. Instead, its oversight is more general and takes the form of what are known as basket warrants. These authorizations can last up to one year. The act does not specify the breadth of the surveillance they can approve, leading some to characterize the authorization as monitoring plans."). The ACLU has brought suit alleging inter alia that the "dragnet" surveillance authorized by the FISA Amendments Act violates the Fourth Amendment. Amnesty et al. v. Blair*: FISA Amendment Act Challenge*, ACLU, Apr. 15, 2010, http://www.aclu.org/national-security/amnesty-et-al-v-blair. The district court dismissed the lawsuit for lack of standing. *See* Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633 (S.D.N.Y. 2009). That judgment is currently on appeal before the Second Circuit.

257. Granting the FISC review of surveillance programs targeting persons outside the United States was a reversal of the general exemption from oversight of such programs that was enacted in the Protect America Act of 2007, Pub. L. No. 110-55, § 105A, 121 Stat. 552, 552 ("Nothing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States."), *amended by* FISA Amendments Act of 2008 § 702, 122 Stat. at 2438–48. Under the FISA Amendments Act, the surveillance may not ordinarily begin until thirty days after the submission to the FISC of the materials certifying that the program is compliant with the requirements of FISA. *See* FISA Amendments Act of 2008 § 702(g)(2)(D), 122 Stat. at 2440–41. Section 702(c)(2), however, provides the Attorney General and the DNI with the authority to begin conducting surveillance prior to the issuance of the FISC's order should they determine that, due to exigent circumstances, "intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order." *Id.* § 702(c)(2), 122 Stat. at 2438. They can do so either prior to submitting the certification of a program to the FISC or while the court is reviewing a program. *Id.* § 702(c)(3), 122 Stat. at 2438. Additionally, the government is permitted to amend the details of previously approved programs and conduct the programs as amended during the period in which the FISC reviews such amendments. *Id.* § 702(i)(1)(C), 122 Stat. at 2443–44.

258. FISA Amendments Act of 2008 § 702(g)(2), 122 Stat. at 2440–41. The government must craft procedures that are designed (1) to ensure that it is only targeting persons outside the United States and to avoid the intentional collection of communications in which both sender and all intended recipients are within the United States; (2) to satisfy minimization requirements as defined by § 101(h) or § 301(4); and (3) to ensure compliance with the requirement that the surveillance neither targets U.S. persons outside the United States nor has the purpose of actually targeting specific persons inside the U.S. *Id.* § 702 (g)(2)(A)–(C), 122 Stat. at 2440.

259. *Id.* § 702(i)(3)(B)(ii), (4)(A), 122 Stat. at 2445. While awaiting a rehearing or an appeal decision, the government may generally continue any of its ongoing programs. *Id.* § 702(i)(4)(B), 122 Stat. at 2445.

260. *See* Camara v. Mun. Court, 387 U.S. 523 (1967) (holding that probable cause for warrants to

new law is that it assigns to the FISC a role in the judicial review of compliance with the terms of basket warrants. This power is, in turn, largely bound up with the FISC's supervision of the government's compliance with its stated plans for targeting foreigners overseas and differentiating potentially valuable intelligence from reams of innocuous information about individuals not suspected of terrorist involvement.[261] (Other parts of the government's certification, such as its general claim that "a significant purpose of the acquisition is to obtain foreign intelligence information,"[262] are likely to be treated deferentially.) As Senator Dianne Feinstein explained during an exchange before the Senate Judiciary Committee, the issuance of programmatic warrants calls for "court oversight," by which the FISC could "set the strictures, say [']I want you to report to me every 3 months, every 30 days,['] [and thus] provide oversight protection."[263]

In other hearings, senior government officials reiterated this role of the FISC in post hoc judicial review. For example, in testimony before the House Judiciary Committee, Assistant Attorney General for National Security Ken Wainstein observed that "[t]he FISA Court is receiving the procedures by which we conduct this surveillance," which places the court in a position to detect a government program, and "that doesn't fit with the law."[264] Opponents of the new law remarked on the departure from

---

enforce the housing code need not require evidence of a violation at a specific location but instead is measured by a reasonableness standard). *See also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (upholding police sobriety checkpoint stops despite a lack of individualized suspicion). *See generally* William C. Banks, *Programmatic Surveillance and FISA—Of Needles and Haystacks*, 88 TEX. L. REV. (forthcoming 2010).

261. *See supra* note 258.

262. FISA Amendments Act § 702(g)(2)(A)(v), 122 Stat. at 2440.

263. *FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 52 (2007) (testimony of Morton H. Halperin, Director of U.S. Advocacy, Open Society Institute). In response to Senator Feinstein, Patrick Philbin, former Deputy Assistant Attorney General, stated, "I think it is certainly an improvement on FISA to ensure that the court can provide programmatic approvals." *Id.* (testimony of Patrick Philbin, former Deputy Assistant Att'y Gen). *See also, e.g.*, *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part I): Hearing Before the H. Comm. on the Judiciary*, 110th Cong. 115 (2007) (testimony of Morton H. Halperin, Director of U.S. Advocacy, Open Society Institute) [hereinafter *Warrantless Surveillance Hearing*] ("The problem comes because the executive branch wants the authority to listen to these calls without a warrant or with a generalized warrant that says you can listen to all the calls, and then what happens if there are a lot of Americans?").

264. *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II): Hearing Before the H. Comm. on the Judiciary*, 110th Cong. 72 (2007) (testimony of Kenneth L. Wainstein, Assistant Att'y Gen.).

historical practice.[265] During congressional debates, Senator Kit Bond, relying on a report issued by the Republicans on the Senate Intelligence Committee, and referring obliquely to the differences between individualized and more aggregative warrants, said:

> [T]he FISA Court has little, if any, historical experience with assessing compliance with minimization in the context of foreign targeting. There are significant differences between the scope, purpose, and means by which the acquisition of foreign intelligence is conducted in the domestic and foreign targeting contexts. While the FISA Court is well-suited to assess compliance with minimization procedures in the domestic context, such assessment is better left to the Executive branch in the foreign targeting context.[266]

How this process has played out in practice is thus far difficult to say.[267] But, especially when viewed in light of the fact that the FISC now receives semiannual reports on the status of collection under program warrants, a new model of judicial review of intelligence programs appears to be emerging: one that assigns to the court a role not only in the ex ante issuance of warrants (even basket warrants), but also in the substantive hard look–style review of agency compliance with stated intelligence programs.[268] Although the court's purview is limited (by the terms of FISA) to the supervision of electronic surveillance conducted by the federal intelligence community,[269] the kind of judicial review that the FISC is now engaged in brings contemporary practice much closer to the sort of judicial review that I advocate.

One major difference between judicial review before the FISC and traditional judicial review of agency action stands out: the absence of a meaningful adversarial process within the intelligence review process.[270] This difference—the result of a structural feature of intelligence

---

265. *See, e.g.*, 154 CONG. REC. S310–14 (daily ed. Jan. 25, 2008) (statement of Sen. Dodd); 153 CONG. REC. S15,722–23 (daily ed. Dec. 17, 2007) (statement of Sen. Feingold).

266. 154 CONG. REC. S6,392 (daily ed. July 8, 2008) (statement of Sen. Bond). To be sure, the Republican report advocated for less FISC governance of basket warrants, not for the undoing of basket warrant authority.

267. *See* Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 16, 2009, at A1 ("The [NSA] intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress last year . . . .").

268. *See, e.g.*, Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29 (1983).

269. *See* 50 U.S.C. § 1803(a)(1) (2006).

270. *Compare* 50 U.S.C. § 1805(a) (directing FISC judge to issue an ex parte order), *with* Administrative Procedure Act, 5 U.S.C. § 702 (2006) (granting any "person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action" the right to "judicial review thereof").

gathering—is at least partially addressed by the FISA Amendments Act in that the law provides for the possibility of judicial review of directives to compel the participation of telecommunications firms in electronic surveillance.[271] Thus, Section 702(h)(6) of the new law authorizes a service provider who receives such a directive to "file a petition with the [FISA] Court of Review," following which "[t]he Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph."[272]

While promising in concept (because telecommunications firms are arguably in a better position than government officials, both technically and institutionally, to uncover potential abuse), and potentially helpful in addressing a constitutional concern pertaining to the absence of a case or controversy before the FISA Court of Review,[273] participation by telecommunications carriers in litigation before the FISC may prove less useful in practice. In a much debated provision, the FISA Amendments Act immunizes telecoms from liability arising from following directives issued from the government,[274] making it unlikely that any communications provider will challenge any directive it receives.[275]

A slightly different, and slightly more promising, approach has recently been explored by the Second Circuit in a case surrounding the use of national security letters ("NSLs")—essentially administrative subpoenas

---

271. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702(h)(4), 122 Stat. 2436, 2441–42 (granting FISC jurisdiction to review petitions from telecommunications firms).

272. *Id.* § 702(h)(6)(A), 122 Stat. at 2443. Litigation of just this sort arose under the Protect America Act, the predecessor to the FISA Amendments Act. That litigation culminated in the FISA Court of Review's opinion in *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008). In a previous appeal before the FISA Court of Review, that court called for and received briefing from numerous public interest–oriented organizations, including the ACLU. *See In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

273. Harold Hongju Koh raised a similar point in testimony before the Senate Judiciary Committee, stating:

> Also curious is the bill's Section 704, which directs the FISA court to consider the benefits of a particular program "as reflected by the foreign intelligence information obtained." This is a judgment, calling in effect for an advisory opinion, which is far more appropriate for a legislative committee than for an Article III court tasked with deciding cases or controversies.

Wartime Executive Power and the National Security Agency's Surveillance Authority II: Hearing Before the S. Comm. on the Judiciary, 109th Cong. (2006) (statement of Harold Hongju Koh, Dean, Yale Law School).

274. FISA Amendments Act of 2008 § 702(h)(3), 122 Stat. at 2441.

275. Even prior to the FISA Amendments Act, only one major telecom was apparently unwilling to assist the government in performing electronic surveillance outside the bounds of FISA. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1. The telecoms cooperated with the government despite a worry about potential criminal liability. *See* 18 U.S.C. § 2511 (2006).

by which the government requests information from providers of telephone or electronic communications services (such as Internet providers).[276] While the original statutory authority for NSLs required that the recipient of such a letter strictly comply with its terms without disclosing to anyone (including counsel) the fact that the letter was received—let alone its contents—a number of district courts found the statute's nondisclosure requirement to violate the First Amendment.[277] Congress subsequently revisited the law in the course of amending the PATRIOT Act and provided for the possibility of judicial review of the NSL's nondisclosure order at the initiation of the letter's recipient.[278] The Second Circuit found that by placing the burden on the recipient to challenge the nondisclosure order, the NSLs continued to run afoul of the First Amendment. Rather than strike down the statute as written, the court came up with a novel remedy.[279] The recipient could merely notify the government of its intent to challenge the nondisclosure requirement, following which the government would be accorded a period of time within which "to initiate a judicial review proceeding to maintain the nondisclosure requirement."[280] While not eliminating the problem of the absence of incentives on the part of third parties to challenge government requests for information (and the corresponding requirement that secrecy be maintained), the Second Circuit approach has the benefit of placing the burden on the government to initiate the proceedings and to overcome a presumption against it.

C. THE *ATTORNEY GENERAL'S GUIDELINES*: PUBLIC PARTICIPATION

Owing to its secretive nature, interest groups are significantly less prominent in the intelligence process than they are across the regulatory state, where legal mechanisms such as informal notice-and-comment rulemaking create meaningful opportunities for pluralist participation. Some modicum of change may be occurring with respect to this critical

276. *See generally* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS (2007) (discussing the history of national security investigations both pre- and post 9/11).

277. *See, e.g.*, Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

278. USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, sec. 3, § 501(f), 120 Stat. 278, 278–79; USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 3511,120 Stat. 194, 211–13 (2006).

279. As the Second Circuit put it in *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 883 (2d Cir. 2008), "We deem it beyond the authority of a court to 'interpret' or 'revise' the NSL statutes to create the constitutionally required obligation of the Government to initiate judicial review of a nondisclosure requirement. However, the Government might be able to assume such an obligation without additional legislation."

280. *Id.* at 879.

feature of regulatory governance. The process by which the new *Attorney General's Guidelines* were issued bore at least a passing resemblance to traditional informal agency rulemaking.[281] FBI general counsel Valerie Caproni recently observed that the new guidelines were "signed after unprecedented consultation"[282] with interest groups, including civil liberties advocates such as the American Civil Liberties Union.[283] She further explained that "historically the Attorney General has not brought Congress or outside groups into the process of drafting guidelines. Having the consultation process is new, and I believe it was extremely helpful."[284]

---

281. 5 U.S.C. § 553 (2006). Thus, Senator Bond asked a senior FBI official, "What opportunity have the outside privacy national security groups had to offer any comments? Do you anticipate any changes based on comments from those groups or from Congress?" The official responded:

> We have held a series of briefings over the last six weeks. We've held three formal briefings to staff up on the Hill. We then also had an extensive briefing session with numerous outside organizations, both civil rights groups and civil liberties and privacy organizations.
>
> We have also made the guidelines available upon request to Members and Committee staff. This has been a six-week process. We do anticipate making changes in response to the comments that we have received.

Attorney General Guidelines Hearing, *supra* note 117, at 18 (testimony of Elisebeth Collins Cook, Assistant Att'y Gen.).

Senator Jay Rockefeller expressed his appreciation at the "Attorney General's decision to consult with Congress and his willingness to seek comments on the proposed guidelines, not only from the Hill, but also from selected representatives of civil liberties organizations on a read and return basis, which has already taken place." *Id*. at 1 (statement of Sen. Jay Rockefeller). He went on to express regret, however, that the guidelines

> have not been publicly released, by which I mean in a broader sense for broader debate and broader comment, not just the people who would cluster about the subject, but broader than that, because this is a huge decision. Circulating the actual proposed guidelines would be a constructive step in generating additional review and commentary.

Id. Soon thereafter the guidelines were, in fact, released publicly.

282. Andrew Kalloch, *FBI General Counsel Defends New Guidelines*, HARV. L. REC., Dec. 4, 2008, http://media.www.hlrecord.org/media/storage/paper609/news/2008/12/04/News/FBI-General.Counsel.Defends.New.Guidelines-3568931.shtml. According to one official, the notice and comment procedure had been employed once before by the FBI. As an unnamed senior official put it,

> I'd like to say this model is not new. During the NSL discussions some time back, when we came out with the FBI guidance to make it clearer for agents in terms of that compliance—these are the touchstones that have to be hit. We brought the same groups in, or many of the same groups, and had them go over the proposed guidance, and they went over it and they came up with a couple of dozen suggested changes. Interestingly, most of what they came up with wasn't, "we don't want you to do this." Most of what they came up with was[,] "what does this mean?" Which was a lot of what the discussion was today. Very similar to this—what exactly does that mean? And when we explained in detail what [we] meant, most of their things—wouldn't it be clearer if you added this or if you said that? And I think the vast majority of what they gave in that, in those discussions, actually got put into the guidance. So, in other words, . . . we looked at it as two things. One, it's the level of transparency. The second thing was it was productive for both of us.

U.S. Dep't of Justice, Briefing with Department Officials on Consolidated Attorney General Guidelines (Sept. 12, 2008) (transcript available at http://www.usdoj.gov/opa/pr/2008/September/08-opa-814.html) (speaker identified as "Senior FBI Official 2").

283. Kalloch, *supra* note 282.

284. *Attorney General Guidelines Hearing*, *supra* note 117, at 9 (testimony of Valerie Caproni,

FBI director Robert Mueller underscored that the FBI not only sought suggestions from outside groups in a spirit of openness that went much further than the sets of guidelines that had gone before, but that the FBI was also incorporating suggestions that were made.[285] Beyond the groups that were present for the consultation process, Mueller committed to making the FBI internal rules issued pursuant to the new guidelines "[publicly] available . . . to the greatest extent possible."[286]

Not everyone was convinced of the adequacy of the new approach. In particular, certain politicians argued for even greater transparency and public participation in the formulation of the new guidelines. Senator Russ Feingold challenged the process, asking Director Mueller during a Senate committee hearing, "Why can't you at least solicit . . . suggestions in a meaningful process that involves more than a single meeting where the participants aren't even allowed . . . to keep a copy [of the draft guidelines]?"[287] Regardless of the fact that it did not represent as robust an instance of popular participation in rulemaking as many would have liked, the process's very existence suggests the possible emergence in the domestic intelligence arena of a new ethic of interest group representation—a hallmark of agency rulemaking across the administrative state for a generation.[288]

General Counsel, FBI). An unnamed senior official explained the process as follows:

> [It's been] a very productive discussion. I think that there is not always going to be agreement between us and other groups . . . to what techniques should be available to investigate threats to . . . national security. There are longstanding and sincerely held beliefs about what are the appropriate restrictions on the FBI's conduct. I hope that we had a good conversation with them and that they would understand where we are coming from. We were not singing Kumbaya when we left the briefing, but we did shake hands and they thanked us for having them in.

Briefing with Department Officials, *supra* note 282.

285. *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 110 Cong. (2008) (testimony of Robert S. Mueller, III, Director, FBI) [hereinafter *Oversight Hearing*].

286. *Id.* at 23. The rules are now posted on the FBI website. *See* DOMESTIC INVESTIGATIONS & OPERATIONS GUIDE (FBI 2008), *available at* http://foia.fbi.gov/foiaindex/diog.htm.

287. Director Mueller responded by noting that "this is the first time, in my experience, that we have sought outside input—not just from Congress, but also from the ACLU, privacy interests, in order to get suggestions." *Oversight Hearing*, *supra* note 285, at 23.

288. *See, e.g.*, *[Errata] Restoring the Rule of Law: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. 428 (2008) (statement of Daniel Farber and Anne Joseph O'Connell, Professors, University of California, Berkeley, School of Law (Boalt Hall)) (stating that "[a]bsent a clear contrary need, every national security policy with consequences for civil liberties and other democratic values should go through notice and comment procedures" (emphasis omitted)).

VI. CONCLUSION

Thinking of domestic intelligence as a form of risk assessment and advocating for a regulatory form of intelligence governance confers a number of benefits. At the conceptual level, these innovations make a significant contribution to solving a problem that has confounded policymakers and commentators for at least a generation: What kind of authority is being exercised when the government engages in domestic intelligence, and how should that authority be constituted and circumscribed? Second, it paves the way for renegotiating social attitudes toward intelligence. As with other powers wielded by the regulatory state, we ought to strive to make domestic intelligence simultaneously more effective and also more honest. Third, and perhaps most significantly, discussion of domestic intelligence as a form of risk assessment and invocation of regulatory processes for governing it pave the way for reframing the national debate about the nature of counterterrorism since 9/11. In place of the familiar war and criminal law paradigms,[289] this Article helps show the way to a risk-management approach to counterterrorism.[290] Counterterrorism is not a matter solely for criminal law enforcement,[291] nor does it necessarily implicate the war powers of the president. Rather, counterterrorism is something different in kind—an approach to managing risk that, in concept, is closely related to other areas of regulatory endeavor.[292] As Paul Bracken recently predicted,

> Whatever direction the Obama administration's national security strategy takes, it will be far more *risk-centric* than the policies of recent years. Risk assessment and management will be central to any American policy because the costs of "winging it," of "going with your gut," have proven to be very high. This reality—the high price of winging it—is the reason other institutions have embraced risk management to improve their performance.[293]

---

289. *See generally* Arunabha Bhoumik, *Democratic Responses to Terrorism: A Comparative Study of the United States, Israel, and India*, 33 DENV. J. INT'L L. & POL'Y 285 (2005) (calling attention to the divergence of the "intelligence" model of counterterrorism from the war and law enforcement models).

290. *See, e.g.*, Roger Cohen, Op-Ed., *After the War on Terror*, N.Y. TIMES, Feb. 8, 2009, *available at* http://www.nytimes.com/2009/01/28/opinion/28iht-edcohen.3.19745699.html?scp=1&sq=cohen%20after%20the%20war%20on%20terror&st=cse (advocating a new approach that would see counterterrorism as a "strategic challenge").

291. *See, e.g.*, Lobel, *supra* note 124.

292. *See* POSNER & VERMEULE, *supra* note 188, at 274 (noting the irony of how academic lawyers who are typically supportive of executive power in the regulation of the economy are typically opposed to it in the context of national security).

293. *See* Paul Bracken, E-Note, *Intelligence and Risk Management*, Dec. 2008, FOREIGN POL'Y

When J. Edgar Hoover presided over the growth of domestic intelligence, his vision was to create a "bureau of intelligence," with its connotation of a New Deal regulatory body steeped in science and expertise.[294] But over time, insufficient oversight and rampant abuses within the intelligence apparatus caused domestic intelligence to lose its technocratic bearings, to the point that by the mid-1970s, criminal law appeared to be the most logical choice for a framework for analyzing and governing domestic intelligence. This Article highlights the possibility of returning domestic intelligence to its regulatory origins and updating that vision to suit the temper of the times. In so doing, it paves the way for reconciling the two great administrative law developments of the last century: the emergence of the New Deal regulatory state and the growth of the Cold War national security apparatus. Domesticated intelligence lies at their intersection.

RESEARCH INST., *available at* http://www.fpri.org/enotes/200812.bracken.intelligencerisk management.html (arguing that risk management has not been widely used in the intelligence community because the intelligence community has historically been unclear how to employ it).

294. *See* KELLER, *supra* note 94, at 13–14.