SHADOW ADMINISTRATIVE CONSTITUTIONALISM AND THE CREATION OF SURVEILLANCE CULTURE

Anjali S. Dalal[*]

2014 MICH. ST. L. REV. 59

TABLE OF CONTENTS

INTRODUCTION 60
I. ADMINISTRATIVE CONSTITUTIONALISM AT WORK 66
A. Surveillance and the Hoover Years 67
B. The *Keith* Case 72
C. Watergate 75
D. *Laird v. Tatum* 76
E. A National Conversation 78
II. SHADOW ADMINISTRATIVE CONSTITUTIONALISM AT WORK ... 83
A. The Reexpansion of the FBI's Mission 84
B. The Reuse of Questionable Methods to Pursue the Mission 88
C. The Recreation of an Intelligence-Gathering Process Cloaked in Secrecy 97
III. NORM ENTREPRENEURSHIP IN THE SHADOWS: THE NATURAL IMPULSE TOWARDS MISSION CREEP 99
A. Powerful, Loosely Defined Mandate 99
B. Medieval Structure of Bureaucracy 102
IV. NORM ENTRENCHMENT IN THE SHADOWS: THE UNWITTING ACCEPTANCE OF AGENCY NORMS INTO CULTURE AND LAW 103
A. How Entrenchment Happens 105

* J.D., Yale Law School; B.A., B.S., University of Pennsylvania. I am indebted to Jack Balkin for his continued guidance and encouragement. Many thanks also to Dru Brenner-Beck, Robert Chesney, Ami Dalal, Chris Donesa, William Eskridge, Linda Greenhouse, Aziz Huq, Margot Kaminski, Jennifer Keighley, Sophia Lee, Theresa Lee, Dan Meyer, Gillian Metzger, Steven Morrison, Lisa Larrimore Ouellette, David Pozen, Michael Traynor, and Andrew Tutt. Thanks also to the participants of the Santa Clara Internet Works in Progress, the Freedom of Expression Conference at Yale Law School, the National Security Law Conference at South Texas School of Law, and the Privacy Law Scholars Conference for their invaluable comments. For unyielding support, I am deeply grateful to Corey Pierson.

B. Surveillance Culture 106
V. CONDITIONS THAT FACILITATE SHADOW ADMINISTRATIVE CONSTITUTIONALISM 114
A. "Super-Deference" 114
B. Secrecy 117
VI. FORCING ADMINISTRATIVE CONSTITUTIONALISM OUT OF THE SHADOWS 118
A. Checks and Balances Within the Executive Branch 118
1. *Interagency Review* 119
2. *Oversight by High-Ranking Officials* 123
3. *Dissent Channel: Whistleblowing* 125
B. Interbranch Deliberation 128
1. *Judicial Intervention* 128
a. Judicially Enforceable Rights 128
b. The Standing Hurdle 129
c. Executive Privilege 132
2. *Congressional Oversight* 133
C. Public Transparency 135
CONCLUSION 136

> *[T]o those who scare peace-loving people with phantoms of lost liberty, my message is this: Your tactics only aid terrorists, for they erode our national unity and diminish our resolve. They give ammunition to America's enemies, and pause to America's friends. They encourage people of good will to remain silent in the face of evil.*[1]

INTRODUCTION

In the wake of what has been called the "biggest intelligence leak" in the National Security Agency's (NSA) history,[2] exposing "dragnet government surveillance"[3] of American communications

1. *Department of Justice Oversight: Preserving Our Freedoms While Defending Against Terrorism: Hearings Before the S. Comm. on the Judiciary*, 107th Cong. 313 (2001) (statement of John Ashcroft, Att'y Gen. of the United States) (emphasis added).

2. *See, e.g.*, Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

3. Joe Mullin, *Anti-Spying Activists Plan Rallies Across US on July 4th Holiday*, LAW & DISORDER/CIVILIZATION & DISCONTENTS (July 2, 2013), http://arstechnica.com/tech-policy/2013/07/anti-spying-activists-plan-rallies-across-us-on-july-4th-holiday/ ("The focus is on changing Section 215 of the Patriot Act,

and the sharing of that communication between agencies, the country convulsed and began discussing drastic measures to rein in surveillance practices: defunding the NSA,[4] repealing § 215 of the PATRIOT Act,[5] and severely limiting the FBI's authority to collect domestic communications under the Foreign Intelligence Surveillance Act (FISA).[6] Months later, the furor has died down, but as new information from Mr. Snowden's massive trove continues to trickle in, there is still discussion of reform, albeit less drastic.[7]

Successful, systemic reform of our surveillance culture requires more than a reflexive response to the latest locus of public outrage; it requires an understanding of the complex conditions that support its existence. This Article suggests that our culture of surveillance is the result of more than just a specific statute or a specific institution. Through a detailed study of the development and evolution of the Attorney General Guidelines, this Article suggests that agencies, engaging in constitutional interpretation with very little oversight or transparency, have shifted the boundaries of acceptable activities and norms regarding domestic surveillance.

---

which is believed to be the legal justification for the dragnet government surveillance uncovered by recent NSA leaks.").

4. Gregory Ferenstein, *The NSA Won a Defunding Battle, but It Could Lose the War*, TECHCRUNCH (July 25, 2013), http://techcrunch.com/2013/07/25/the-nsa-won-yesterdays-battle-but-it-could-lose-the-war/ ("Yesterday, July 24th, the House of Representatives nearly ratified the most brazen amendment to completely cut off funds for any broad NSA spying program (failing 205-217)." (emphasis omitted)).

5. Stephen Dinan, *Top Senator Calls for Scrapping Key Snooping Patriot Act Section*, WASH. TIMES (Sept. 24, 2013), http://www.washingtontimes.com/news/2013/sep/24/sen-leahy-scrap-key-patriot-act-section/?page=all.

6. Pete Kasperowicz, *Leahy Offers Bill to Sunset FISA Provisions*, HILL (June 24, 2013), http://thehill.com/blogs/floor-action/senate/307423-bipartisan-senate-group-proposes-patriot-act-fisa-reforms.

7. Charlie Savage, *Obama to Call for End to N.S.A.'s Bulk Data Collection*, N.Y. TIMES (Mar. 24, 2014), http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?_r=2; Josh Gerstein, *Obama Plans New Limits on NSA Surveillance*, POLITICO (Dec. 5, 2013), http://www.politico.com/politico44/2013/12/obama-plans-new-limits-on-nsa-surveillance-178986.html (quoting President Obama as stating, "'I'll be proposing some self-restraint on the NSA[. A]nd . . . to initiate some reforms that can give people more confidence.'" (quoting Interview by Chris Matthews with Barack Obama, President of the United States, on *Hardball with Chris Matthews* (MSNBC television broadcast Dec. 5, 2013), *available at* http://www.nbcnews.com/id/53755285/ns/msnbc-hardball_with_chris_matthews/#.UwEPTF 5-imE)).

As a number of academics have noted, agencies are increasingly involved in the business of constitutional interpretation.[8] This aspect of agency life has been termed "administrative constitutionalism." Administrative constitutionalism is a type of extra-judicial constitutionalism that focuses on the role of agencies in constitutional interpretation. It is an instantiation of popular constitutionalism that views agencies as the front line of constitutional interpretation, taking the first shot at implementing congressional statutes and applying judicial doctrine.

Administrative constitutionalism has been championed by academics as an important and underexplored aspect of constitutional interpretation.[9] Professor Sophia Lee, for example, has

---

8. For example, the Department of Justice (DOJ), in coordination with the Pentagon and the State Department, determines the constitutional boundaries of drone warfare. *See infra* note 269 and accompanying text. The U.S. Patent and Trademark Office broadly interprets the scope of patentability as provided by its governing statutes and the U.S. Constitution. *See, e.g.*, Wm. Redin Woodward, *A Reconsideration of the Patent System as a Problem of Administrative Law*, 55 HARV. L. REV. 950 (1942). And, as Gillian Metzger has recently noted, "The Department of Education and the Department of Justice (DOJ) jointly issue guidance explaining how elementary and secondary schools can voluntarily consider race consistently with governing constitutional law." Gillian E. Metzger, *Administrative Constitutionalism*, 91 TEX. L. REV. 1897, 1897 (2013).

9. *See, e.g.*, Metzger, *supra* note 8, at 1898 (arguing that "instances of administrative constitutionalism are a frequent occurrence, reflecting the reality that most governing occurs at the administrative level and thus that is where constitutional issues often arise" (footnote omitted)); WILLIAM N. ESKRIDGE JR. & JOHN FEREJOHN, A REPUBLIC OF STATUTES: THE NEW AMERICAN CONSTITUTION 1 (2010); Sophia Z. Lee, *Race, Sex, and Rulemaking: Administrative Constitutionalism and the Workplace, 1960 to the Present*, 96 VA. L. REV. 799, 804 (2010) (documenting the FCC and FPC "administrators' interpretation of several aspects of equal protection—primarily the state action doctrine, affirmative equality rights, and affirmative action—to show how they advanced constitutional policies that imaginatively extended or retracted, increasingly diverged from, and even contradicted courts' constitutional doctrine" (footnote omitted)); Gillian E. Metzger, *Ordinary Administrative Law as Constitutional Common Law*, 30 J. NAT'L ASS'N ADMIN. L. JUDICIARY 421, 427 (2010) ("Recognizing the interrelationship between constitutional law and ordinary administrative law is important both for the ongoing debate over the legitimacy of constitutional common law and for the proper appreciation of the role administrative agencies can play in our constitutional order."); Reuel E. Schiller, *Free Speech and Expertise: Administrative Censorship and the Birth of the Modern First Amendment*, 86 VA. L. REV. 1, 15-18, 27-28 (2000) (examining how the de facto role agencies play in statutory interpretation gives agencies a de facto role in determining the scope of First Amendment protections); Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 568-69 (2007) (describing how Congress and the Post Office developed communications privacy based on

provided one of the first detailed factual account of the interpretative practices of the Federal Communications Commission and the Federal Power Commission, demonstrating that agencies are actively engaged in constitutional interpretation.[10]

Professors Bill Eskridge and John Ferejohn build upon this descriptive account and argue that agencies are and *should be* constitutional norm entrepreneurs.[11] In their view, new constitutional norms are like "trial balloons hoisted by agencies . . . subject to public critique as well as veto by courts, legislatures, and other executive branch officials."[12] This interbranch, intergovernmental, and public deliberation, Eskridge and Ferejohn argue, is the "dominant governmental mechanism for the evolution of America's fundamental normative commitments."[13] The dialogic process leads to consensus around these proposed norms that reflects public opinion and political compromise. The consensus around these norms then slowly becomes entrenched, and such entrenched norms, Eskridge and Ferejohn argue, should be respected by the Supreme Court.

Eskridge and Ferejohn further claim that this process of small-"c" constitutionalism is a superior way to ascribe meaning to the big-"C" Constitution, finding that "it is more adaptable to changed circumstances . . . [and] is more legitimate than the Constitutional updating that unelected judges routinely accomplish in the default of a workable Constitutional amendment process."[14] Administrative constitutionalism, so understood, posits as its central claim that

---

extra-constitutional principles later adopted by the Supreme Court in their Fourth Amendment jurisprudence).

10. *See* Lee, *supra* note 9, at 800-01, 803-04.

11. Norms are traditionally distinguished from legal rules on a number of dimensions, but the central distinction is that "norms are enforced by some means other than legal sanctions." *See, e.g.*, Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 350 (1997). As reviewed and synthesized in McAdams's article, the scholarship exploring the interaction between law and norms is extensive and interdisciplinary, with economists, sociologists, and legal academics all having contributed to the study of the origin and function of norms. *See generally id.* In this Article, norms are used to describe those principles and policies that are reflected in and embraced by the electorate, regardless of legal sanction. However, the process of norm entrepreneurship and entrenchment, as explored later in this Paper, is oftentimes intertwined with the creation of laws, regulations, or non-legally binding internal guidelines.

12. ESKRIDGE & FEREJOHN, *supra* note 9, at 33.

13. *Id.*

14. *Id.* at 18.

administrative agencies should regularly engage in constitutional norm entrepreneurship, beginning a process of national deliberation that results in the entrenchment of norms that reflect the majority viewpoint.

This Article builds upon the work of these scholars. Through a historical and analytical study of the development and evolution of the Attorney General Guidelines, the governing document for the FBI, this Article demonstrates that agencies, in their role as norm entrepreneurs, can also engage in what I call "shadow administrative constitutionalism"—a process of agency-norm entrepreneurship and entrenchment that occurs *without* the necessary public consultation, deliberation, and accountability. Furthermore, this Article identifies the hospitable conditions of the national security arena that support shadow administrative constitutionalism. While these conditions may prove commonplace and not unique to the national security arena, such an analysis is beyond the scope of this Article.

The evolution of the Attorney General Guidelines suggests that the deliberation that Eskridge and Ferejohn demand in response to agency norm entrepreneurship naturally occurs only in those rare instances when we find ourselves in a national conversation—when the entire country is galvanized around a major reinterpretation of our rights framework. Outside of these moments, our national security institutions are insular organizations often operating under the radar of meaningful checks and balances. They operate with an institutional proclivity towards mission creep and the norms developed become entrenched through a process of path-dependency and faith in historical practice. This corrupted process of agency norm entrepreneurship and entrenchment is what I call shadow administrative constitutionalism. It is a process in which agency norm entrepreneurship does not reflect public values and is not met with the dialogic process assumed by Eskridge and Ferejohn, but nevertheless leads to the entrenchment of norms that are far from democratically obtained. Furthermore, I argue that shadow administrative constitutionalism in the national security arena is inevitable without the manufactured interventions of deliberation-forcing mechanisms.

The Article proceeds in six parts. Part I provides a snapshot of agency norm entrepreneurship that demonstrates the power and promise of administrative constitutionalism. This Part traces the growth of the FBI's domestic surveillance program from its early years until the country was forced into a national conversation on the government surveillance norms that had emerged over the greater

part of the twentieth century. In response to this national conversation, the DOJ developed the first-ever Attorney General Guidelines to govern the FBI's domestic surveillance activity. The Guidelines, known as the Levi Guidelines,[15] represented a model instance of agency norm entrepreneurship. By striking a balance between national security needs and civil-liberties guarantees that reflected the tenor of the time, the Levi Guidelines provide an excellent example of agency norm entrepreneurship and a positive snapshot of administrative constitutionalism.

Part II provides an account of shadow administrative constitutionalism at work. This Part details the historical evolution of the Guidelines and the reemergence of surveillance norms. This reemergence suggests a weakness of administrative constitutionalism in practice: after the dust settles and our collective attention begins to fade, agencies continue to actively engage in norm entrepreneurship, but now they do so within the isolated echo chambers of the agencies themselves.

Parts III and IV together explore the rationale behind and consequence of the norms developed in the account of shadow administrative constitutionalism provided in Part II. Part III attributes the instinct toward aggressive national security norms to the powerful, loosely defined nature of the national security mandate and the medieval structure of bureaucracy. Part IV discusses the process by which norms become entrenched in shadow administrative constitutionalism through its two component parts: path dependency and faith in historical practice. Part IV closes with a discussion of the consequence of this account of shadow administrative constitutionalism: surveillance culture. Together, Parts III and IV illustrate that, without the necessary oversight and deliberation, administrative constitutionalism can morph from a powerfully democratic approach to defining the values that bind our country to an illegitimate process by which the bureaucratic impulses of unelected agency actors slowly shape our values and our law.

Part V studies the features of policymaking in the national security arena that inhibit oversight and deliberation. In particular, this Part posits that the "super-deference" granted agencies in charge of national security issues and the secrecy under which national

15. The Levi Guidelines were named after then Attorney General Edward Levi. Letter from Edward H. Levi, Att'y Gen. of the United States, to Clarence M. Kelley, Dir., FBI (Nov. 4, 1976), *reprinted in FBI Statutory Charter: Hearings Before the S. Comm. on the Judiciary*, 95th Cong. 18 (1978) [hereinafter Levi Guidelines].

security must necessarily operate makes oversight and deliberation particularly difficult.

Part VI identifies the weak internal and external checks and balances that further facilitated shadow administrative constitutionalism and suggests structural solutions to improve the oversight and deliberation necessary to ensure the legitimacy of administrative constitutionalism.

I. ADMINISTRATIVE CONSTITUTIONALISM AT WORK

The Administrative State can be a powerful democratic force in the process of constitutional interpretation. This Part provides a snapshot of administrative constitutionalism at its best: an agency engaging in norm entrepreneurship as part of a broader national conversation regarding how to define the scope of civil-liberties protections in the context of national security threats. It moves in three Sections. First, it provides a brief account of the J. Edgar Hoover years at the FBI, with a particular focus on the years spanning between World War II and the early 1970s. This Section illustrates the three dominant, problematic features of the Hoover FBI: the unrestrained expansion of the FBI's mission, the pursuit of the mission through illegal means, and the creation of an intelligence-gathering process cloaked in secrecy. Second, I describe the momentous year of 1972, when three important incidents—the *Keith* case,[16] Watergate, and *Laird v. Tatum*[17]—brought the issue of domestic surveillance to a head and launched a national debate about how to both protect civil liberties and national security. Third, I describe the norm entrepreneurship that followed, where the Department of Justice, drawing from the tone and tenor of the national conversation and the recommendations of a congressional investigatory committee, introduced the Attorney General Guidelines to govern the FBI—a proposed method of striking that difficult balance between preserving civil liberties and national security. These Guidelines provide a perfect snapshot of the first stage of administrative constitutionalism, norm entrepreneurship, at work.

16. United States v. U.S. District Court (*Keith*), 407 U.S. 297 (1972).
17. 408 U.S. 1 (1972).

A. Surveillance and the Hoover Years

For nearly five decades, J. Edgar Hoover's name was synonymous with the FBI. He came to the FBI as its founding Director and left it only in death, after forty-eight years of service.[18] The Hoover years covered an incredibly tumultuous time in the country's history: over the course of his tenure, the United States experienced Prohibition, the growth of organized crime, World War II, the Cold War, the Civil Rights Movement, and the Korean and Vietnam Wars. By some measures, it was during Hoover's tenure that the country first began to need a federal investigative body to protect the country from domestic and international threats.

Though the FBI was originally created as a federal investigative body to aid in the prosecution of federal crimes, World War II expanded the FBI's mandate to include surveillance for national security purposes.[19] The original order from President Roosevelt to J. Edgar Hoover in 1934 was simply to conduct a one-time investigation of the Nazi movement within the United States; however, two years later, Roosevelt asked for a more "systematic collection of intelligence" about Fascism and Communism.[20] By the end of World War II, the intelligence apparatus was equipped with "bureaucratic momentum" and had gained public acceptance as a "substantial permanent intelligence system."[21]

Furthermore, during the Hoover Years, the modern conception of a powerful, unitary executive emerged from "the retention of powers accrued during the emergency of World War II."[22] One such power was the executive authority used to establish and sustain the

18. While the FBI was only formally created in 1935, its predecessor organization was the Bureau of Investigation for which Hoover was the director beginning May 10, 1924. *See A Brief History of the FBI*, FBI, http://www.fbi.gov/about-us/history/brief-history (last visited Mar. 14, 2014). The forty-eight-year term of service includes Hoover's time as Director of the Bureau of Investigation and the FBI. *See John Edgar Hoover*, FBI, http://www.fbi.gov/about-us/history/directors/hoover (last visited Mar. 14, 2014).

19. *See A Brief History of the FBI*, *supra* note 18.

20. *See* S. REP. NO. 94-755, bk. II, at 25 (1976). This paper draws on many of the factual details and findings of this study of U.S. intelligence activities conducted by the U.S. Senate, which was led by Senator Frank Church. By its own account, this study "conducted the only thorough investigation ever made of United States intelligence and its post World War II emergence as a complex, sophisticated system of multiple agencies and extensive activities." *Id.* bk. I, at 7.

21. *Id.* at 9-10.

22. *Id.* at 10.

intelligence community during World War II.[23] When initially petitioning for an expansion of the FBI's intelligence-gathering mandate on the eve of World War II, Hoover contended that the FBI Appropriations Act passed during World War I already authorized the proposed expansion.[24] However, "[t]here [was] no evidence that either the Congress in 1916 or Attorney General Stone in 1924 intended the provision of the appropriations statute to authorize the establishment of a permanent domestic intelligence structure."[25] Nevertheless, to maintain his agency's intelligence authorities as World War II loomed on the horizon, Hoover advised Attorney General Homer Cummings and President Franklin Roosevelt in 1938 that the 1916 appropriations statute that applied to the World War I-era intelligence program was "'sufficiently broad'" to allow the President to "expan[d] . . . the present intelligence and counter-espionage work" as "deemed necessary" by the executive branch.[26] As the Church Committee later discovered, because both Roosevelt and Cummings wanted to keep the intelligence program secret and wished to avoid a consultation with Congress on the matter, neither man questioned Hoover's interpretation of the statute and Roosevelt signed an executive order authorizing domestic intelligence-gathering activity in anticipation of World War II.[27]

In 1939, President Roosevelt issued another directive, which "was the closest thing to a formal charter for FBI and military domestic intelligence."[28] It was three paragraphs long and simply stated that "'investigation of all espionage, counterespionage, and sabotage matters be controlled and handled by the Federal Bureau of Investigation'" in coordination with the Intelligence Divisions of the Army and Navy.[29] With that, a formal intelligence-gathering program was instituted in the United States at the behest of the President.[30] This three-paragraph "charter" was the FBI's central form of governance until the intelligence reforms of the 1970s.[31] As a result,

23. *Id.*
24. *Id.* bk. II, at 28-29.
25. *Id.* bk. III, at 400.
26. *Id.*
27. *Id.*; *see also* TIM WEINER, ENEMIES: A HISTORY OF THE FBI 80 (2013).
28. S. REP. NO. 94-755, bk. III, at 402.
29. *Id.* at 403 (quoting a confidential memorandum from the President).
30. *See id.*
31. *Id.* at 548-49 (describing the testimony of Assistant Attorney General Robert Mardian in March of 1971 that "neither the Department nor the Bureau had 'any specific published regulation or guideline' for the collection of intelligence

national security remained predominantly under the purview of the executive branch, with intelligence agencies continuing to report directly to the President and operating with immense authority and little oversight.[32]

Finally, during Hoover's tenure, the country began to witness the development of powerful monitoring and surveillance equipment as a result of the research and development and capacity-building efforts that came with World War II and the subsequent arms race of the Cold War. For example, the Strategic Arms Litigation Talks (SALT) negotiations of the late 1960s and the treaties that emerged were "possible because technological advances ma[d]e it possible to accurately monitor arms limitations" remotely.[33] As later noted by the congressionally appointed Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more commonly known as the "Church Committee" for its Chairman, Senator Frank Church, these "technological innovations . . . markedly increased the agencies' intelligence collection capabilities."[34]

These characteristics of the post-World War II era proved to be particularly hospitable to the growth of an underground but powerful domestic surveillance regime. For example, these conditions allowed for the development of the infamous Counterintelligence Program (COINTELPRO). COINTELPRO was created to target the "Communist threat" in the United States, but, soon, "the program widened to other targets, increasingly concentrating on domestic dissenters."[35] Between 1956 and 1971, the program actively "'disrupt[ed]' groups and 'neutralize[d]' individuals deemed to be threats to domestic security."[36]

Importantly, COINTELPRO "was not designed to build traditional cases to be brought to trial"; rather, the program was developed in response to the FBI's "frustrat[ion] with Supreme Court limits on overt investigations of dissident groups" such as the

---

about civil disturbances") Indeed, the investigations were "based on the 1939 Roosevelt directives." *Id.*

32. *See id.*

33. *Id.* bk. I, at 10.

34. *Id.*

35. *Id.* bk. II, at 65; *see also* JEROME P. BJELOPERA, CONG. RESEARCH SERV., R41780, THE FEDERAL BUREAU OF INVESTIGATION AND TERRORISM INVESTIGATIONS 24 (2013), *available at* http://www.fas.org/sgp/crs/terror/R41780.pdf.

36. S. REP. NO. 94-755, bk. II, at 10; *see also* WEINER, *supra* note 27, at 195, 292-93.

Socialist Workers Party, the Ku Klux Klan, the New Left, and the Black Panther Party.[37] The constitutional limits on government surveillance placed by the Supreme Court led the FBI to conduct surveillance in secret and in a manner that intentionally avoided judicial review.[38]

COINTELPRO ultimately extended its purview to include all "'person[s] who trie[d] to arouse people to violent action by appealing to their emotions, prejudices, et cetera,'" and, once identified, such persons were placed on the FBI's "Rabble Rouser Index," later renamed the "Agitator Index."[39] This list targeted a number of nonviolent civil rights organizations including the Southern Christian Leadership Conference.[40] The Church Committee later determined that FBI Headquarters had developed over 500,000 domestic intelligence files on Americans and domestic groups, including the NAACP, the Women's Liberation Movement, and Conservative American Christian Action Council.[41] COINTELPRO embodied the FBI's disregard for civil liberties. It targeted individuals and organizations precisely because of their First Amendment-protected political speech and associational activity.

COINTELPRO illustrates the three prominent features of the Hoover FBI: the unrestrained expansion of the FBI's mission, the pursuit of mission through illegal means, and the creation of an intelligence-gathering process cloaked in secrecy.

First, with Hoover at the helm, the FBI gradually expanded its mission from strictly federal law enforcement,[42] to domestic intelligence gathering for wartime national security, and finally to

---

37. BJELOPERA, *supra* note 35, at 24; *see also* S. REP. NO. 94-755, bk. II, at 67.

38. BJELOPERA, *supra* note 35, at 24.

39. S. REP. NO. 94-755, bk. II, at 90 (quoting the 1967 FBI Rabble Rouser Index).

40. BJELOPERA, *supra* note 35, at 24.

41. S. REP. NO. 94-755, bk. II, at 6-8.

42. The FBI was limited to federal law enforcement in its early days in part because of the scandal caused by the "Palmer Raids" of the 1920s. ALPHEUS THOMAS MASON, HARLAN FISKE STONE: PILLAR OF THE LAW 113-14 (1956). Responding to the mass arrests of innocent individuals, Attorney General Harlan Fiske Stone limited the Bureau of Investigation, which preceded the FBI, to the investigation of federal crimes. *See id.* at 150. Stone ordered Hoover, then Acting Director of the Bureau, to limit the work of the FBI "'strictly to investigations of violation of law, under my direction or under the direction of an Assistant Attorney General regularly conducting the work of the Department of Justice.'" *Id.* at 151 (quoting a 1924 memorandum from U.S. Attorney General Harlan F. Stone to J. Edgar Hoover).

domestic intelligence gathering to preserve social and political order within the United States. "The absence of precise standards for intelligence investigations" in part led to this overgrowth.[43] As the Church Committee later found, intelligence standards and limitations set out by Attorney General Harlan Fiske Stone after World War I were abandoned by the FBI in favor of internally issued mandates to investigate "'subversion'"—a term that remained undefined—and "'potential' rather than actual or likely criminal conduct, as well as [mandates] to collect general intelligence on lawful political and social dissent."[44]

Second, without guidelines defining the boundaries of acceptable activity, the FBI pursued its mission through a number of illegal methods.[45] This included targeting individuals, organizations, and ideologies in violation of the First Amendment and the equal protection guarantees of the Constitution.[46] Furthermore, as part of COINTELPRO and other agency initiatives, FBI agents illegally opened the private mail of American citizens, intercepted their cables, and wiretapped and bugged their private conversations without judicial warrant.[47] Armed with this trove of private information, the FBI deployed it for political purposes: to mail anonymous letters to break up marriages, air the political beliefs of individuals to get them fired from their jobs, and falsely label members of organizations as government informants in order to discredit them within their respective organizations or expose them to violent attack.[48] When asked about the FBI's mail opening program, one former FBI official justified this illegal behavior by explaining that "'[i]t was my assumption that what we were doing was justified by what we had to do . . . [for] the greater good, the national security.'"[49]

Third, the FBI was able to sustain its illegal activity by operating under a veil of secrecy. President Roosevelt authorized this secrecy in his August 1936 directive establishing the basic domestic intelligence structure in the United States when he made clear that

43. S. REP. NO. 94-755, bk. II, at 165.
44. *Id.*
45. *Id.* at 12.
46. *Id.* at 12-13.
47. *Id.*
48. *Id.* at 10-11.
49. *Id.* at 14 (quoting the testimony of W.A. Branigan).

the domestic intelligence plan to be handled "quite confidentially."[50] This sentiment was later echoed by Hoover when he stated that "'the expansion of the present structure of intelligence work . . . [should] proceed[] . . . with the utmost degree of secrecy in order to avoid criticism or objections which might be raised to such an expansion by either ill-informed persons or individuals having some ulterior motive.'"[51] Hoover further added, "'[I]t would seem undesirable to seek any special legislation which would draw attention to the fact that it was proposed to develop a special counterespionage drive of any great magnitude.'"[52] The Hoover FBI, operating under the "fear of war, and its attendant uncertainties and doubts, ha[d] fostered a series of secret practices that ha[d] eroded the processes of open democratic government."[53]

The Hoover FBI was finally reined in when, in 1972, three major incidents forced a national conversation about domestic surveillance and intelligence-gathering practices: the Supreme Court decision in *United States v. U.S. District Court*, also known as the *Keith* case, a case that addressed the illegal wiretapping of Americans;[54] the Watergate break-in; and the Supreme Court decision in *Laird v. Tatum*, a case that addressed First Amendment issues arising from Army surveillance of Americans during the Race Riots of the 1960s.[55]

B. The *Keith* Case

The case arose from the "dynamite bombing of a Central Intelligence Agency ('CIA') recruitment office . . . in Ann Arbor, Michigan" on September 29, 1968.[56] Though no one was injured, the

50. *Id.* bk. III, at 392 (quoting a Confidential Memorandum by J. Edgar Hoover dated August 25, 1936, describing President Roosevelt's approach to the proposed domestic intelligence-gathering program).

51. *Id.* (quoting a letter from Attorney General Homer Cummings to President Roosevelt).

52. *Id.* (quoting a letter from Attorney General Homer Cummings to President Roosevelt).

53. *Id.* bk. I, at 9.

54. 407 U.S. 297, 299 (1972).

55. 408 U.S. 1, 3-5 (1972).

56. The Historical Society for the United States District Court for the Eastern District of Michigan provides a useful history describing the event that led up to the momentous case. *See* Samuel C. Damren, *The* Keith *Case*, CT. LEGACY, (Historical Soc'y for the U.S. Dist. Court for the E. Dist. of Mich., Detroit, Mich.), Nov. 2003, at 1, 1, *available at* http://www.mied.uscourts.gov/HistoricalSociety/media/newsletters/200311_Court_

blast left a twelve-inch-by-seven-inch-wide and six-inch-deep reminder in the sidewalk of the social unrest in the country.[57] John Sinclair, Laurence Robert "Pun" Plamondon, and John "Jack" Waterhouse Forest, "all members of the radical White Panther Party," were indicted, and Judge Damon Keith was appointed to preside over the case.[58]

"On October 5, 1970, the defense filed a [routine] motion for the disclosure of electronic surveillance" conducted on the defendants.[59] "In response to the motion, the prosecution and defense" agreed to a stipulation in which "the prosecution represented to the court that it had no knowledge of any electronic surveillance of the defendants and that the local office of the FBI was also unaware of any electronic surveillance."[60] The national offices of the FBI, however, had conducted electronic surveillance of one of the defendants. At this point, Attorney General Mitchell informed the court that government agents had tapped defendant Plamondon in the course of its efforts to gather intelligence on domestic organizations that were deemed "subversive" and a potential threat to the government.[61]

Then, as the Historical Society for the United States District Court for the Eastern District of Michigan reports, "the government filed a motion to dismiss the defendants' request for disclosure of the surveillance evidence[,] . . . certif[ying] that public disclosure of the facts concerning surveillance of the defendants would prejudice the national interest."[62] Furthermore, the government requested it "be notified prior to any decision requiring disclosure of the surveillance so that it could determine whether to proceed with the case."[63]

Judge Keith rejected the government's request and, in doing so, rejected the "'Mitchell Doctrine,' which asserted that the Attorney General, as a representative of the executive branch, had the inherent constitutional power both to authorize electronic surveillance in 'national security' cases without judicial warrant and to unilaterally determine whether a particular circumstance falls within the scope of

---

Legacy.pdf. "The bombing was one of eight anti-establishment bombings that had occurred in the Detroit area at the time." *Id.*

57. *Id.*
58. *Id.* at 1-2.
59. *Id.* at 4.
60. *Id.* at 5.
61. *Id.*
62. *Id.*
63. *Id.*

a 'national security' concern."[64] As a consequence, Judge Keith found himself the subject of a mandamus suit.[65]

In 1972, the mandamus suit reached the Supreme Court, and the Court formally rejected the Mitchell Doctrine and affirmed Judge Keith's position that, while there is a constitutional basis for the President's domestic security efforts, "it must be exercised in a manner compatible with the Fourth Amendment."[66] *Keith* held that under the particular circumstances presented, the government was required to obtain a warrant prior to engaging in electronic surveillance of Americans on American soil.[67] In doing so, the Court also recognized that other procedures might also be constitutionally legitimate depending on the circumstances presented.[68] Specifically, the Court recognized that "the focus of domestic surveillance may be less precise than that directed against more conventional types of crime" and that, as such, Congress might deem it necessary to apply different standards to domestic surveillance not conducted in pursuit of a crime already governed by the Wiretap Statute.[69] At the same time, however, the Court recognized that the need for extra flexibility in national security-motivated domestic surveillance is counterbalanced by the fact that such cases "often reflect a convergence of First and Fourth Amendment values *not* present in cases of 'ordinary' crime."[70]

The Court further emphasized that 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.'"[71] Writing for the Court, Justice Powell rung a warning bell, reminding us that

> [t]he price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[72]

64. *Id.*
65. United States v. U.S. District Court (*Keith*), 407 U.S. 297 (1972).
66. *Id.* at 320.
67. *Id.* at 321-22.
68. *Id.* at 322-23.
69. *Id.* at 322.
70. *Id.* at 313 (emphasis added).
71. *Id.* at 314.
72. *Id.*

C. Watergate

On June 17, 1972, two days before *Keith* was decided, the Watergate break-in occurred.[73] While the Watergate break-in and the bugging of the Democratic Party Headquarters was just one of many instances of the "political spying and sabotage conducted on behalf of President Nixon's re-election,"[74] the incident was key to exposing the systematic and illegal surveillance practices.

As the celebrated reporters Woodward and Bernstein reported, "hundreds of thousands of dollars in Nixon campaign contributions had been set aside to pay for an extensive undercover campaign aimed at discrediting individual Democratic presidential candidates and disrupting their campaigns."[75] The campaign

> included[f]ollowing members of Democratic candidates' families and assembling dossiers on their personal lives; forging letters and distributing them under the candidates' letterheads; leaking false and manufactured items to the press; throwing campaign schedules into disarray; seizing confidential campaign files; and investigating the lives of dozens of Democratic campaign workers.[76]

The Nixon Administration had gone so far as to break into a psychiatrist's office to obtain the medical history of Daniel Ellsberg, the former defense analyst who leaked the Pentagon Papers, in order to discredit him.[77] As one former Nixon staffer described:

> [Nixon] ordered me and the others, a group that would come to be called the "plumbers," to find out how the leak had happened and keep it from happening again. Mr. Hunt urged us to carry out a "covert operation" to get a "mother lode" of information about Mr. Ells-berg's mental state, to discredit him, by breaking into the office of his psychiatrist, Dr. Lewis Fielding. Mr. Liddy told us the F.B.I. had frequently carried out such covert operations—a euphemism for burglaries—in national security investigations, that he had even done some himself.[78]

---

73. Alfred E. Lewis, *5 Held in Plot to Bug Democrats' Office Here*, WASH. POST (June 18, 1972), http://www.washingtonpost.com/wp-dyn/content/article/2002/05/31/AR2005111001227.html.

74. Carl Bernstein & Bob Woodward, *FBI Finds Nixon Aides Sabotaged Democrats*, WASH. POST (Oct. 10, 1972), http://www.washingtonpost.com/politics/fbi-finds-nixon-aides-sabotaged-democrats/2012/06/06/gJQAoHIJJV_story.html.

75. *Id.*

76. *Id.*

77. Egil Krogh, Op-Ed., *The Break-In That History Forgot*, N.Y. TIMES (June 30, 2007), http://www.nytimes.com/2007/06/30/opinion/30krogh.html.

78. *Id.*

The Watergate scandal placed on public display both the extent of and abuse of domestic surveillance activities by the executive branch.

D. *Laird v. Tatum*

In the same year *Keith* was decided, the Supreme Court considered the constitutionality of the Army's surveillance of American citizens in *Laird v. Tatum*.[79] The case stemmed from a program in which President Lyndon Johnson ordered the Army to assist local authorities in managing the riots springing up across the country after the assassination of Dr. Martin Luther King Jr. in 1967.[80] In this capacity, the Army began a data gathering effort in order to facilitate "more detailed and specific contingency planning designed to permit the Army, when called upon to assist local authorities, to be able to respond effectively with a minimum of force."[81]

The data-gathering effort consisted of the United States Army collecting information on citizens and civil rights organizations by surreptitiously attending public meetings and culling information from newspapers to identify flashpoint issues, planned protest activities, and key persons within the organizations.[82] Furthermore, the Army maintained political files on prominent public officials holding office in the United States Congress.[83] The rationale provided for this surveillance, as the Court of Appeals observed, was that, because "the Army is sent into territory almost invariably unfamiliar to most soldiers and their commanders, their need for

---

79. 408 U.S. 1, 2 (1972).

80. *Id.* at 4-5. The President couched his authority to order such a program in 10 U.S.C. § 331 (2006), which states:

> Whenever there is an insurrections [sic] in any State against its government, the President may, upon the request of its legislature or of its governor if the legislature cannot be convened, call into Federal service such of the militia of the other States, in the number requested by that State, and use such of the armed forces, as he considers necessary to suppress the insurrection.

10 U.S.C. § 331; *see also Tatum*, 408 U.S. at 3-4.

81. *Tatum*, 408 U.S. at 5.

82. *Id.* at 6.

83. Files were maintained on Senator Adlai E. Stevenson III and Congressman Abner J. Mikva. S. REP. NO. 94-755, bk. II, at 8 (1976); *see also* George C. Christie, *Government Surveillance and Individual Freedom: A Proposed Statutory Response to* Laird v. Tatum *and the Broader Problem of Government Surveillance of the Individual*, 47 N.Y.U. L. REV. 871, 872 (1972).

information is likely to be greater than that of the hometown policeman."[84]

The plaintiffs in *Tatum* were "four individuals and nine unincorporated associations engaged in lawful political activity, including but not limited to union organizing, public speaking, peaceful assembly, petitioning the government, newspaper editorializing, and educating the public about political issues."[85] The plaintiffs alleged that their constitutionally protected expressive activities were subject to unlawful monitoring by the Army, thereby chilling their ability to speak freely.[86]

The Court dismissed the case, holding that the plaintiffs did not present a justiciable controversy because they did not show evidence of an *objective harm* or the threat of a *specific future harm*.[87] The Court refused to recognize the plaintiffs' allegations of a "subjective chill" on their speech arising "merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual."[88] Thus, plaintiffs alleging harms of free speech and association resulting from a publicly known domestic surveillance program operated by the U.S. government must put forth evidence that *they themselves* were the subjects of said surveillance and, further, that the surveillance created an objective harm in order for a constitutional challenge to the surveillance to be considered justiciable. In so holding, the Court overturned the lower court's more liberal construction of the standing requirement requiring only a "*likelihood*

84. Tatum v. Laird, 444 F.2d 947, 952-53 (D.C. Cir. 1971), *rev'd*, 408 U.S. 1 (1972).

85. Brief for Respondents at 4, *Tatum*, 408 U.S. 1 (No. 71-288).

86. *Id.* at 2-3.

87. *See Tatum*, 408 U.S. at 3 ("We granted certiorari to consider whether, as the Court of Appeals held, respondents presented a justiciable controversy in complaining of a 'chilling' effect on the exercise of their First Amendment rights where such effect is allegedly caused, not by any 'specific action of the Army against them, [but] only [by] the existence and operation of the intelligence gathering and distributing system, which is confined to the Army and related civilian investigative agencies.' We reverse." (alteration in original) (citation omitted) (quoting *Tatum*, 444 F.2d at 953)).

88. *Id.* at 11.

that [the surveillance] will affect" the exercise of First Amendment rights.[89]

Tatum made clear that while government surveillance was indeed a problem facing the American public, the courts were not going to be quick to intervene.

E. A National Conversation

With *Keith*, Watergate, and *Tatum* all coming to a head in 1972, the country was quickly forced into a national dialogue about the constitutional boundaries of executive power, the scope of the national security mandate, and the appropriateness of domestic intelligence gathering. To both represent and inform the public in this conversation, a special committee was created by Congress and tasked with the job of assessing the intelligence-gathering practices of the government. This committee became known as the "Church Committee" under the chairmanship of Senator Frank Church, and in 1976, it published the "Church Committee Report."[90] The scathing report famously found that "[t]oo many people have been spied upon by too many Government agencies and to [sic] much information has beeen [sic] collected."[91]

The Church Committee made two important findings. First, that the surveillance program had "adversely affected the constitutional rights of particular Americans," resulting in a harm that "extend[ed] far beyond the citizens directly affected."[92] The Committee was concerned that "[w]ithout clear limits, a federal investigative agency would 'have enough on enough people' so that 'even if it does not elect to prosecute them' the Government would . . . still 'find no opposition to its policies.'"[93] Second, the Church Committee attributed the radical growth of surveillance programs to a failure of our system of checks and balances. As the Committee noted, "In the field of intelligence those restraints have too often been ignored."[94] The Committee attributed this imbalance to: (1) the growth of presidential power, particularly in the area of intelligence

89. Davis v. Ichord, 442 F.2d 1207, 1214 (D.C. Cir. 1970) (emphasis added).

90. *See* S. REP. NO. 94-755, bk. I, at ii (1976).

91. *Id.* bk. II, at 5.

92. *Id.* at 290.

93. *Id.* at 291 (quoting ROBERT H. JACKSON, THE SUPREME COURT IN THE AMERICAN SYSTEM OF GOVERNMENT 71 (1955)).

94. *Id.*

gathering; (2) the veil of secrecy under which domestic intelligence-gathering operations were occurring; and (3) the immunization of the intelligence community from the restraints of the rule of law.[95]

The Church Committee provided ninety-six recommended reforms to the intelligence-gathering operations.[96] The reforms focused on creating clear prohibitions against government intelligence gathering that directly infringes the rights of free speech and association; ensuring that any governmental action that affects free speech meets the strict scrutiny standard; and developing procedural safeguards, or so-called "'auxiliary precautions,'" to provide a redundancy to all substantive prohibitions.[97] The procedural checks suggested included "judicial review of intelligence activity before or after the fact, . . . formal and high level Executive branch approval," more disclosure to the public, and "more effective Congressional oversight."[98] Recognizing the limits of its authority to execute upon any these recommendations, the Church Committee urged, "Congress to turn its attention to legislating restraints upon intelligence activities which may endanger the constitutional rights of Americans."[99]

Responding to national concern and the Church Committee's findings, Attorney General Edward Levi, engaging in norm entrepreneurship, issued a set of internal guidelines for FBI investigations in 1976. These guidelines set forth principles and processes that would regulate the FBI's domestic security operations, including its domestic intelligence-gathering efforts.[100] The Levi Guidelines embraced a number of different solutions for how to better balance national security interests with First Amendment guarantees.

---

95. *Id.* at 292.

96. *Id.* at 296-339.

97. *Id.* at 293 (quoting THE FEDERALIST NO. 51, at 291 (James Madison) (Glazier & Co. 1826)).

98. *Id.*

99. *Id.* at 289.

100. Levi Guidelines, *supra* note 15, at 18-33. The Attorney General Guidelines have since expanded to include guidance information on the use of confidential informants, undercover operations, and consensual monitoring guidelines. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES 1 (2005) [hereinafter OIG INVESTIGATION], *available at* http://www.justice.gov/oig/special/0509/final.pdf.

For example, under the Levi Guidelines, domestic security investigations were restricted to ascertaining information on the activities of individuals or groups

> which involve or will involve the use of force or violence and which involve or will involve the violation of federal law, for the purpose of:
>
> (1) overthrowing the government of the United States or the government of a State;
>
> (2) substantially interfering, in the United States, with the activities of a foreign government or its authorized representatives;
>
> (3) substantially impairing for the purpose of influencing U.S. government policies or decisions:
>
> (a) the functioning of the government of the United States;
>
> (b) the functioning of the government of a State; or
>
> (c) interstate commerce;
>
> (4) depriving persons of their civil rights under the Constitution, laws, or treaties of the United States.[101]

These regulations placed a blunt, clear limit on the scope of the FBI's domestic intelligence-gathering authority.

Another such solution was the creation of tiers of FBI domestic security investigations to ensure that breadth of investigative authority granted to FBI agents bore some relationship to predicate factual evidence provided to trigger the investigation. Specifically, the Levi Guidelines created three tiers of investigations—preliminary, limited, and full—each with different attendant authorities, factual requirements, and approvals.[102] For example, a full investigation required "specific and articulable facts giving reason to believe that an individual or a group is or may be engaged in activities which involve the use of force or violence."[103] Comparatively, preliminary investigations needed only "allegations or other information that an individual or a group may be engaged in activities which involve or will involve the use of force or

101. Levi Guidelines, *supra* note 15, at 20.

102. OIG INVESTIGATION, *supra* note 100, at 36-37.

103. Levi Guidelines, *supra* note 15, at 22; *see also* OIG INVESTIGATION, *supra* note 100, at 37; ALLAN ADLER, CTR. FOR NAT'L SEC. STUDIES, A REPORT COMPARING THE PROPOSED FBI CHARTER ACT OF 1979 WITH ATTORNEY GENERAL LEVI'S DOMESTIC SECURITY GUIDELINES, THE RECOMMENDATIONS OF THE CHURCH COMMITTEE, AND OTHER PROPOSALS TO REGULATE FBI INVESTIGATIVE ACTIVITIES 8-9 (1979).

violence."[104] As a result of the higher factual predicate requirements, full investigations were conducted with a broader set of investigative tools than preliminary or limited investigations. However, despite being subject to the lowest standard, preliminary investigations conducted under the Levi Guidelines still required some factual predicate in order to proceed.[105]

Finally, and perhaps most importantly, the Levi Guidelines recognized that domestic security investigations, by their very nature, threatened to chill speech. Accordingly, the Levi Guidelines predicated full investigative authority on the balancing of four factors: "(1) the magnitude of the threatened harm; (2) the likelihood it will occur; (3) the immediacy of the threat; and (4) the *danger to privacy and free expression posed by a full investigation*."[106] Thus, the Guidelines explicitly limited the circumstances that called for domestic intelligence gathering and further limited the initiation of an investigation if the negative impact on First Amendment rights outweighed the value of the surveillance.

In the course of implementing the Levi Guidelines, FBI Director Clarence M. Kelley further contributed to this spate of norm entrepreneurship by "shift[ing] supervision of domestic terrorism investigations from the FBI's Intelligence Division to its Criminal Investigative Division."[107] The Criminal Investigative Division was charged with investigating potential suspects up until the point of the decision to prosecute.[108] This mandate was fundamentally different from the mandate of intelligence gathering, which often lacked a

---

104. Levi Guidelines, *supra* note 15, at 20; *see also* ADLER, *supra* note 103, at 1.

105. As John Elliff explains, prior to 1976, preliminary inquiries were used recklessly, to the point where

> [i]n some cases, the FBI opened preliminary inquiries not only in response to allegations, but also as a means of screening all individuals in a suspect class. For example, the FBI opened preliminary inquiries about all black student leaders in 1971 to determine which of them belonged to groups like the Black Panther Party.

John T. Elliff, *The Attorney General's Guidelines for FBI Investigations*, 69 CORNELL L. REV. 785, 805 (1984) (citing S. REP. NO. 94-755, bk. III, at 527 (1976)); *see also* S. REP. NO. 97-682 app. D at 504 (1983) ("[I]ndividuals and organizations should be free from law enforcement scrutiny that is undertaken without a valid factual predicate and without a valid law enforcement purpose.").

106. Levi Guidelines, *supra* note 15, at 22 (emphasis added); *see also* ADLER, *supra* note 103, at 9; Elliff, *supra* note 105, at 798.

107. Elliff, *supra* note 105, at 794.

108. *Id.* at 795.

clear target or time frame controlling the investigation.[109] By treating domestic security investigations like traditional criminal law enforcement investigations, the DOJ offered one more mechanism to limit the FBI's domestic intelligence-gathering authority.

The impact of these changes was immediately felt. The number of FBI domestic security investigations decreased from 21,414 in July 1973 to 4,868 in March 1976.[110]

The Levi Guidelines were the perfect example of administrative constitutionalism at work. In the context of an active national dialogue, the Levi Guidelines issued a directive that put forth a new set of constitutional norms around government surveillance that responded to general concerns and specific problems, and, most importantly, provided an opportunity to test run solutions and experiment with new norms.[111]

Eskridge and Ferejohn find value in administrative constitutionalism because it facilitates a process of norm development and entrenchment that is gradual and iterative. As they describe, "normative commitments are announced and entrenched not through a process of Constitutional amendments or Supreme Court pronouncements but instead through the more gradual process of legislation, administrative implementation, public feedback, and legislative reaffirmation and elaboration."[112]

---

109. *Id.*

110. OIG INVESTIGATION, *supra* note 100, at 38 (citing CHAIRMAN OF THE SUBCOMM. ON SEC. & TERRORISM, 98TH CONG., 1ST SESS., IMPACT OF ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC SECURITY INVESTIGATIONS (THE LEVI GUIDELINES) 5 (Comm. Print 1984)).

111. There are alternate theories of the motivating intent of the Levi Guidelines. Some have described the Guidelines as "intended . . . to diminish the perceived need for legislation to regulate and restrict" FBI activity. United States v. Salemme, 91 F. Supp. 2d 141, 190 (D. Mass. 1999); *see also* Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. (forthcoming 2014). Even accepting this as true, it does not cut against the central point of the Eskridge and Ferejohn theory of administrative constitutionalism: agencies, as norm entrepreneurs, should attempt to identify and implement emerging national consensus and, in doing so, begin the process of trial and error that will ultimately help locate the national consensus and articulate the rules that best reflect that position. Furthermore, such an alternate interpretation identifies a separate problem with administrative constitutionalism: agency action can be wielded to usurp political momentum and strategically avoid legislation, effectively securing administrative constitutionalism's place in the shadows. If, in practice, legislative action is halted by agency intervention, the role of agencies as appropriate norm entrepreneurs is fundamentally called into question. Further exploration of this point is beyond the scope of this Paper, but I thank Aziz Huq for raising it.

112. ESKRIDGE & FEREJOHN, *supra* note 9, at 14 (emphasis omitted).

In this case, the Levi Guidelines were the first step in such an iterative process. They reflected an administrative agency responding to a national outcry by crafting regulations that reflected the findings and recommendations of a Congress that was in the process of developing legislation to regulate the domestic intelligence gathering. In many instances, the Levi Guidelines adopted legislative proposals that were under consideration, providing a laboratory-like environment in which to test out proposed solutions. This reflected Eskridge and Ferejohn's idealized role of the agency, conforming their policy choices as "rationally consistent with the policy choices already made by a past Congress or likely to be acceptable to the current or a future one" given their position as unelected, unappointed actors in this dialogic process.[113]

It is from this high point of an administrative agency productively engaged in the constitutional process that we move to Part II, which details the subsequent history of the Attorney General Guidelines and the regrowth of domestic surveillance activities after 1976.

II. SHADOW ADMINISTRATIVE CONSTITUTIONALISM AT WORK

After the Levi Guidelines were issued, legislation both authorizing and regulating the FBI stalled, leaving the Attorney General Guidelines as the central source of governance for the FBI.[114] Moreover, since the creation of the Levi Guidelines, there has been a steady unmooring of the Attorney General Guidelines from the rights-protecting framework enshrined in 1976. This unmooring suggests a weakness of administrative constitutionalism in practice: after the dust settles and our collective attention begins to fade, an agency shifts to shadow administrative constitutionalism. In this new phase, an agency continues to actively engage in norm entrepreneurship, but, instead of drawing from a national

113. *Id.* at 16.

114. As Professor John Elliff explains in his excellent study of the early iterations of the Attorney General Guidelines:

> In the absence of an explicit legislative charter, the FBI derives its statutory mandate primarily from the Attorney General's authority to appoint officials: "(1) to detect and prosecute crimes against the United States; (2) to assist in the protection of the person of the President; and (3) to conduct such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General."

Elliff, *supra* note 105, at 786 (quoting 28 U.S.C. § 533 (1976)).

conversation to identify potential norms, an agency now draws from within the isolated echo chambers of the agency itself.

From 1976 to date, there have been six notable developments to the Attorney General Guidelines under Attorneys General Civiletti, Smith, Thornburgh, Reno, Ashcroft, and Mukasey. Each iteration marks a slow, steady drift away from the substantive and procedural limitations placed on the domestic intelligence-gathering activities of the FBI. The result is that the hallmarks of the FBI are once again an unregulated expansion of its mission, the pursuit of its mission through illegal or potentially illegal means, and the creation of an intelligence-gathering process cloaked in secrecy.

A. The Reexpansion of the FBI's Mission

Since the Levi Guidelines were first put in place, virtually every subsequent administration has revised the Guidelines. The first such change occurred under Attorney General Benjamin R. Civiletti in 1980.[115]

Under the Civiletti Guidelines, the term "criminal intelligence" was created to serve a distinct investigative purpose from the FBI's general crimes investigations.[116] Criminal intelligence applied to FBI investigations "undertaken to obtain information concerning enterprises which are engaged in racketeering activities involving violence, extortion or public corruption" and those "undertaken for the purpose of obtaining information on activities that threaten the national security."[117] Such criminal intelligence investigations stood apart from general crimes investigations, which were conducted to "detect, prevent[,] and prosecute specific violations of federal law."[118]

The creation of a criminal intelligence authority expanded the FBI's intelligence-gathering authority. Criminal intelligence investigations were broader in scope than general crimes investigations and could be authorized for indefinite time frames. As Professor Elliff explains:

> [A]n investigation of a completed criminal act is normally confined to determining who committed that act and with securing evidence to establish the elements of the particular crime. . . . An investigation of an

115. S. REP. NO. 97-682 app. D at 516 (1983).

116. *Id.* at 505.

117. *Id.*; *see also* Elliff, *supra* note 105, at 794.

118. S. REP. NO. 97-682 app. D at 505; *see also* Elliff, *supra* note 105, at 794.

> ongoing criminal enterprise must determine the size and composition of the group involved, its geographic dimensions, its past acts and intended criminal goals, and its capacity for harm. . . . [T]he investigation of a criminal enterprise does not necessarily end, even though one or more of the participants may have been prosecuted.[119]

In 1983, under Attorney General William French Smith, the Guidelines expanded the primary role of the FBI to include domestic security as a separate mission, in addition to criminal law enforcement.[120] Furthermore, the Smith Guidelines expanded the circumstances authorizing a domestic security investigation. Specifically, under the Smith Guidelines, such an investigation was now authorized when "'facts or circumstances [that] reasonably indicat[ed] that two or more persons [were] engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States.'"[121] This language authorized FBI investigations well in advance of any specific crime being contemplated, let alone committed. As Professor Elliff recounts, under these guidelines, "the threshold requirement was 'not expressed . . . in terms of . . . probabilities or degrees of certainty that individuals or organizations are engaged or have engaged in crime'"; rather, the standard simply required "'a reasonable indication that the enterprise to be investigated is organized for the purpose of achieving its ends through criminal activity.'"[122]

---

119. Elliff, *supra* note 105, at 795 (quoting 125 CONG. REC. 21,395, 21,513 (1979)).

120. WILLIAM FRENCH SMITH, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS (1983) [hereinafter SMITH GUIDELINES]; OIG INVESTIGATION, *supra* note 100, at 47.

121. OIG INVESTIGATION, *supra* note 100, at 48 (quoting SMITH GUIDELINES, *supra* note 120, § III.B.1.a); *see also* Elliff, *supra* note 105, at 798.

122. Elliff, *supra* note 105, at 799 (first alteration in original) (quoting Letter from Robert A. McConnell, Assistant Att'y Gen. for Legislative Affairs, to Senator Walter D. Huddleston (Apr. 7, 1983) (on file with Cornell Law Review)); *see also* SMITH GUIDELINES, *supra* note 120, § III.B.1.a. Elliff does not find so wide a gulf between the domestic terrorism investigations parameters under Attorneys General Levi and Smith. He argues:

> The differences between the political or social goals of criminal violence and the purposes for criminal violence enumerated in the Levi guidelines do not mean that the scope of investigations under the Smith guidelines is wider; the broadest purpose in the Levi guidelines was to investigate all individuals and groups that may be engaged in activities that involve or will involve the use of force or violence in violation of federal law for the purpose of "depriving persons of their civil rights."

The Smith Guidelines were drafted in part as a response to a hearing and study conducted by the Senate Subcommittee on Security and Terrorism in the early 1980s, which found the operative Guidelines to be unduly restrictive.[123] The subcommittee concluded that the Guidelines should

> be revised to delete the criminal standard for initiating domestic security investigations; extend time limits for investigations, particularly those for preliminary and limited investigations; lower the evidentiary threshold for initiating limited investigations; relax restrictions on the recruitment and use of new informants; and authorize investigations of systematic advocacy of violence, alleged anarchists, or other activities calculated to weaken or undermine federal or state governments.[124]

In addition to recommending that "the revised Guidelines be tested and evaluated," the Subcommittee recommended that the DOJ "should thereafter 'present legislative recommendations to Congress to justify the enactment into law of adequate and effective guidelines for domestic security investigations.'"[125] Responding to this call, Attorney General Smith issued a revised, more aggressive set of Guidelines, intended "'to ensure protection of the public from the greater sophistication and changing nature of domestic groups that are prone to violence.'"[126]

While this history might suggest the DOJ was operating in active dialogue with Congress instead of in the shadows, I believe it provides, at most, a blip in the otherwise isolated process of norm entrepreneurship and entrenchment engaged in by the Department of Justice. Furthermore, unlike the Levi Guidelines, which were developed by an agency responding to the public and findings of a full-scale congressional investigation, the Smith Guidelines were developed in response to the recommendations of one subcommittee within one house of Congress. To the extent that agencies are to respond to the policy choices "already made by a past Congress or likely to be acceptable to the current or a future one,"[127] the Smith

---

Elliff, *supra* note 105, at 799 (footnote omitted) (quoting Levi Guidelines, *supra* note 15, at 20). However, I respectfully disagree for the reasons stated above.

123. OIG INVESTIGATION, *supra* note 100, at 46.

124. *Id.*

125. *Id.* (quoting CHAIRMAN OF THE SUBCOMM. ON SEC. & TERRORISM, 98TH CONG., 1ST SESS., IMPACT OF ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC SECURITY INVESTIGATIONS (THE LEVI GUIDELINES) 35 (Comm. Print 1984)).

126. *Id.* at 47 (quoting *Attorney General's Guidelines for Domestic Security Investigations (Smith Guidelines): Hearing Before the Subcomm. on Sec. & Terrorism of the S. Comm. on the Judiciary*, 98th Cong. app. A at 47 (1983)).

127. ESKRIDGE & FEREJOHN, *supra* note 9, at 16.

Guidelines reflected an agency responding to a small segment of Congress, a segment that may well have been voicing a minority viewpoint.

The repositioning of the FBI as both a federal law enforcement agency as well as a domestic intelligence-gathering organization was thoroughly entrenched by 2002 when, in response to a country deeply shaken by the September 11 attacks on the World Trade Center and the Pentagon, Attorney General John Ashcroft issued a new set of guidelines that made clear that "the prevention of terrorist acts became the central goal of the law enforcement and national security mission of the FBI."[128]

Responding to what felt like an existential threat to the country, the Ashcroft Guidelines granted incredible power to the FBI. The Guidelines intended to "free the field agents . . . from the bureaucratic, organizational, and operational restrictions and structures that hindered them from doing their jobs effectively."[129] Without the benefit of public debate or congressional input on the way in which the FBI's role needed to be expanded, Ashcroft unilaterally removed barriers that had previously "bar[red] FBI field agents from taking the initiative to detect and prevent future terrorist acts unless the FBI learns of possible criminal activity from external sources."[130] The conception of the FBI as a federal law enforcement agency was long gone, and in its place was an institution dedicated to the prevention of domestic terrorist attacks.

The shift of the FBI's mission from reactive criminal law enforcement to proactive terrorism prevention was affirmed, and explicitly stated, in 2008, when Attorney General Michael Mukasey issued Guidelines that provided the "latest step in moving beyond a reactive model (where agents must wait to receive leads before acting) to a model that emphasizes the early detection, intervention, and prevention of terrorist attacks and other criminal activities."[131] To implement this mission, the Mukasey Guidelines created a new type of inquiry, an Assessment, which, unlike all other previous investigative actions by the FBI, needs no factual predicate for its

---

128. John Ashcroft, Att'y Gen. of the United States, Remarks on the Attorney General Guidelines (May 30, 2002), http://www.fas.org/irp/news/2002/05/ag053002.html.

129. *Id.*

130. *Id.*

131. Press Release, U.S. 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.

initiation.[132] Assessments only require an authorized purpose: that they be "carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence."[133] An FBI agent conducting an Assessment can investigate any individual she chooses based solely on instinct so long as she is carrying out the Assessment in an effort to obtain information about past, present, or future federal crimes or a threat to national security.

In the course of fifty years, the FBI reexpanded from an agency enforcing federal law to an agency protecting against all actual and unlikely threats to our national security. The reexpanded FBI mission is uncomfortably reminiscent of the seemingly endless purview of the FBI under Hoover's tenure.

B. The Reuse of Questionable Methods to Pursue the Mission

By the time the Smith Guidelines were issued in 1983, the FBI's mandate was not the only thing that had morphed. The Smith Guidelines began to change the way FBI investigations were conducted, and the new methods that were authorized began to encroach on civil liberties.

For example, the Smith Guidelines lowered the barrier for initiating a full investigation from one that required "specific and articulable facts" to one that merely required a "reasonable indication" of harm.[134] The boundaries of reasonable indication are vague; it is less rigorous than the specific and articulable facts standard, but also requires more than "a mere hunch."[135] This lower standard was originally proposed in the FBI Charter Bill of 1979, a bill that was introduced and the subject of many hearings, but never made it out of committee.[136] The Smith Guidelines, without

132. MICHAEL B. MUKASEY, OFFICE OF THE ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 19 (2008) [hereinafter MUKASEY GUIDELINES], *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf.

133. *Id.*

134. *See* Levi Guidelines, *supra* note 15, at 22; SMITH GUIDELINES, *supra* note 120, § II.C.1; *see also* OIG INVESTIGATION, *supra* note 100, at 48; Elliff, *supra* note 105, at 799.

135. SMITH GUIDELINES, *supra* note 120, § II.C.1; *cf.* S. REP. NO. 97-682 app. D at 507 (1983).

136. *FBI Charter Act of 1979: Hearing on S. 1612 Before the S. Comm. on the Judiciary*, 96th Cong., pt. 2, at 436-37 (1980); *see also* Elliff, *supra* note 105, at 799.

subjecting itself to the veto gates of the congressional process, ultimately adopted the very standard that was unable to garner the necessary votes to make it out of committee.

The Smith Guidelines also removed the distinction between "preliminary" and "limited" investigations and, in doing so, allowed the FBI to use the same techniques in all investigatory activities that did not qualify as full investigations. Thus, the facts and approvals necessary to begin a preliminary investigation were now sufficient to conduct a limited investigation with its attendant authorities.[137]

Additionally, unlike the Levi Guidelines, the Smith Guidelines allowed FBI agents to attend religious gatherings and public political meetings undercover.[138] In 1983, this authority was at least limited by two factors: first, undercover activity that threatened to influence the free exercise of First Amendment-protected rights needed approval from FBI Headquarters, and second, the FBI was required to notify the DOJ of such undercover activity.[139] By 2003, as discussed in more detail later, these limitations were removed.[140]

Finally, the Smith Guidelines created a provision that authorized the FBI to investigate individuals based on statements that "advocate criminal activity."[141] Specifically, the provision provided that, "[i]n its efforts to anticipate or prevent crime, the FBI must at times initiate investigations in advance of criminal conduct."[142] The Guidelines acknowledged the provision's encroachment on First Amendment-protected activity, though only prohibited investigations that were "based *solely* on activities protected by the First

---

137. *See* SMITH GUIDELINES, *supra* note 120, § II.B.1; *see also* Allison Jones, *The 2008 FBI Guidelines: Contradiction of Original Purpose*, 19 B.U. PUB. INT. L.J. 137, 145 (2009).

138. SMITH GUIDELINES, *supra* note 120, § IV.B.3; *see also* OIG INVESTIGATION, *supra* note 100, at 49.

139. SMITH GUIDELINES, *supra* note 120, § IV.B.3; *see also* OIG INVESTIGATION, *supra* note 100, at 49.

140. *See infra* notes 153-65 and accompanying text; JOHN ASHCROFT, OFFICE OF THE ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATION 22 (2002) [hereinafter ASHCROFT GUIDELINES], *available at* https://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf; *see also* Memorandum from Marvin J. Johnson, Legislative Counsel, ACLU, Interested Persons Memo: Analysis of Changes to Attorney General Guidelines (June 6, 2002), *available at* http://www.aclu.org/print/national-security/interested-persons-memo-analysis-changes-attorney-general-guidelines.

141. SMITH GUIDELINES, *supra* note 120, § I.

142. *Id.*

Amendment."[143] "[S]tatements advocat[ing] criminal activity or indicat[ing] an apparent intent to engage in crime, particularly crimes of violence," would be sufficient to start an investigation unless it was clear that the statements in question did not present a prospect of harm.[144] This language places the responsibility on the individual to make clear that her speech is within the protections of the First Amendment.

In early 1988, five years after the Smith Guidelines were passed, it was discovered that, beginning in 1981, the FBI opened a criminal investigation of the Committee in Solidarity with the People of El Salvador (CISPES), a United States-based group that opposed the Reagan Administration's policies in Central America.[145] The discovery came when a long-time FBI informant alleged that the FBI broke into the Dallas headquarters of CISPES and "wiretapped its members' phones and kept 'terrorist' files on almost 700 people, including two U.S. senators, a House member and a former

143. *Id.* (emphasis added).

144. *Id.* John Elliff provides a fascinating account of litigation that arose as a result of this provision. He writes:

> Shortly after issuance of the Smith guidelines, the U.S. District Court for the Northern District of Illinois ruled that the new guidelines conflicted with a settlement reached in earlier litigation that established standards for FBI domestic security investigations in Chicago. The settlement had incorporated the Levi guidelines and stated that the FBI "'shall not conduct an investigation solely on the basis of activities protected by the First Amendment.'" Citing the Supreme Court's decision in *Brandenburg v. Ohio*, the district court interpreted "activities protected by the First Amendment" as including advocacy that is not "'directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action.'" Concluding that the provision in the new guidelines authorizing investigation when "statements advocate criminal activity" permitted investigations that may not meet the *Brandenburg* test, the court enjoined implementation of the Smith guidelines within Chicago. The district court based its ruling on the terms of the 1981 settlement, not on a determination that the Smith guidelines were unconstitutional. The court expressed no opinion on the merits of the constitutional argument that an activity protected from criminal sanctions may not be protected from the "more limited" power to investigate.

Elliff, *supra* note 105, at 808-09 (alteration in original) (footnotes omitted). The Seventh Circuit affirmed the decision; however, the injunction was lifted as "unnecessary." *Id.* at 809 (citing Alliance to End Repression v. City of Chicago, 733 F.2d 1187, 1192 (7th Cir. 1984)).

145. *See, e.g.*, Philip Shenon, *F.B.I. Papers Show Wide Surveillance of Reagan Critics*, N.Y. TIMES, Jan. 28, 1988, at A1, *available at* http://www.nytimes.com/1988/01/28/us/fbi-papers-show-wide-surveillance-of-reagan-critics.html.

ambassador."[146] Congressional inquiries and investigative reports followed. The FBI's own internal investigation showed that "the FBI had conducted an appropriate investigation for the initial period, but that its objectives became overly broad when FBI Headquarters directed all offices to treat each of the estimated 180 chapters of CISPES as subjects of the investigation."[147] The House Judiciary Committee's report extended beyond just a review of the CISPES incident and included a review of FBI investigative practices in general. The report found:

- [T]he FBI closed approximately 67 percent of its investigations because it did not develop evidence indicating that the subjects were engaging in international terrorist activities;
- United States citizens and permanent resident aliens were the subject of 38 percent of the 18,144 cases opened during January 1982-June 1988;
- mosques were among the religious institutions targeted in the 1980s investigations; and
- the FBI monitored First Amendment-related activities in about 11.5 percent of those cases; indexed information about individuals who were not subjects of FBI investigations in about 47.8 percent of the cases; and indexed information about groups which were not subjects of the investigations in about 11.6 percent of the cases.[148]

Despite these findings, no modifications on the FBI's investigatory methods and procedures were made. Emphasizing both how increasingly detached from and immune to public outcry the FBI had become, the CISPES scandal did not catalyze any significant change to the Attorney General Guidelines governing the FBI.[149] Instead, the Guidelines issued in March 1989 were minor and dealt largely with approval authority for preliminary inquiries.[150]

---

146. Eric Pianin, *U.S. Behind Break-Ins, Sanctuary Leaders Testify*, WASH. POST, Feb. 20, 1987, at A27.

147. OIG INVESTIGATION, *supra* note 100, at 51.

148. *Id.* at 53-54. For more information, see U.S. GEN. ACCOUNTING OFFICE, GAO/GGD-90-112, INTERNATIONAL TERRORISM: FBI INVESTIGATES DOMESTIC ACTIVITIES TO IDENTIFY TERRORISTS app. I at 28-30 (1990), *available at* http://www.gao.gov/assets/150/149691.pdf.

149. If press reports are any indication, there was significant public pressure to reform intelligence activity after the CISPES scandal. *See, e.g.*, Charles R. Babcock, *FBI Surveillance of Policy Critics Alleged*, WASH. POST, Feb. 13, 1987, at A34; Philip Shenon, *F.B.I.'s Chief Says Surveillance Was Justified*, N.Y. TIMES, Feb. 3, 1988, at A1, *available at* http://www.nytimes.com/1988/02/03/us/fbi-s-chief-says-surveillance-was-justified.html; Sanford J. Ungar, *The F.B.I. on the Defensive Again*, N.Y. TIMES (May 15, 1988),

The next update to the FBI's investigative methods came with Attorney General Reno. Instead of additional substantive changes, the Reno Guidelines further entrenched existing standards. After both the 1993 attack on the World Trade Center and the 1995 attack on the Alfred P. Murrah federal building, FBI capability to detect and prevent acts of terrorism came under fire.

As a result, in November 1995 the Reno Guidelines were issued which, while maintaining the general language around investigatory methods, provided a more detailed interpretation of the existing Guidelines, emphasizing that the "'reasonable indication' standard for opening a full investigation is 'substantially lower than probable cause' and that a preliminary investigation could be opened on a lesser showing."[151]

The next set of major changes came in response to the September 11 attacks and further lowered barriers to begin investigations. Attorney General Ashcroft explained:

> "Under the current guidelines, FBI investigators cannot surf the web the way you or I can. Nor can they simply walk into a public event or a public place to observe ongoing activities. They have no clear authority to use commercial data services that any business in America can use. These restrictions are a competitive advantage for terrorists who skillfully utilize sophisticated techniques and modern computer systems to compile information for targeting and attacking innocent Americans."[152]

To address this frustration and make intelligence gathering easier more generally, the Ashcroft Guidelines instituted four significant changes.

First, as mentioned earlier, the Ashcroft Guidelines authorized the FBI to engage in surveillance of public gatherings and meetings

---

http://www.nytimes.com/1988/05/15/magazine/the-fbi-on-the-defensive-once-again.html.

150. OIG INVESTIGATION, *supra* note 100, at 53 n.135.

151. *Id.* at 56 (quoting a memorandum circulated to FBI field offices).

152. *Id.* at 188-89 (quoting Ashcroft, *supra* note 128). Ashcroft's claims were not entirely accurate; the FBI was authorized to do all three of those activities pursuant to an ongoing investigation, as Ashcroft himself noted in later testimony in front of the Senate Judiciary Committee. There he explained that the FBI was authorized to engage in the aforementioned activities so long as it was pursuant to an existing criminal investigation. *Oversight of the Dept. of Justice: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. (2002) (statement of John Ashcroft, Att'y Gen. of the United States), *available at* http://www.fas.org/irp/congress/2002_hr/072502ashcroft.html; *cf. supra* note 126 and accompanying text.

without any checks or balances.[153] While the Smith Guidelines already allowed "'undisclosed participation in the activities of an organization by an undercover employee or cooperating private individual in a manner that may influence the exercise of rights protected by the First Amendment,'"[154] such surveillance required approval. In particular, before agents were authorized to surreptitiously attend religious gatherings or associational meetings, they needed approval from FBI headquarters and the DOJ.[155] Under the Ashcroft Guidelines, authorization from FBI Headquarters was no longer needed, and the DOJ was no longer notified. Instead, the FBI was given blanket authority "to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally," as long as they enter said place "[f]or the purpose of detecting or preventing terrorist activities."[156] As the ACLU noted at the time, this rationale sounds uncomfortably similar to the rationale used by the FBI in order to send "agents into churches and other organizations during the civil rights movement . . . to block the movement, suppress dissent, and protect the administration."[157]

---

153. *See supra* note 140 and accompanying text; *see also infra* Subsection VI.A.2.

154. OIG INVESTIGATION, *supra* note 100, at 49 (quoting SMITH GUIDELINES, *supra* note 120, § IV.B.3).

155. SMITH GUIDELINES, *supra* note 120, § IV.B.3.

156. ASHCROFT GUIDELINES, *supra* note 140, at 22. Part VI "explicitly authorizes the FBI to visit public places and attend public events on the same terms and conditions as members of the public for the purpose of detecting or preventing terrorist activities." OIG INVESTIGATION, *supra* note 100, at 11. Originally, under the Levi Guidelines, "the FBI's authority to engage in these activities generally was interpreted to be limited to the investigation of crimes or the collection of criminal intelligence only when agents had a sufficient evidentiary basis to check leads, conduct a preliminary inquiry, or conduct a full investigation." *Id.*

157. Memorandum from Marvin J. Johnson, *supra* note 140. Interestingly, a request for this type of information was made earlier in the FBI's history, but at that time, to no avail. In 1982, FBI Director William H. Webster expressed frustration with having to conform to the data-gathering provisions of the recently passed Privacy Act of 1974. He complained of the agency's "inability to review periodicals or other publications of organizations that are not under investigation," a limitation that prohibits agencies from collecting and maintaining records on how individuals or organizations exercise their First Amendment rights unless it pertains to an active investigation. *Domestic Security (Levi) Guidelines: Hearings Before the Subcomm. on Sec. & Terrorism of the S. Comm. on the Judiciary*, 97th Cong. 12 (1983) (statement of William H. Webster, Director, FBI). As a result, Webster sounded the call, to be repeated often until Ashcroft successfully changed the rules, that "it makes little sense to deny us information that is available to the general public." *Id.*

Second, the Ashcroft Guidelines authorized the FBI to purchase detailed profiles compiled by data mining companies without any evidence supporting suspicion.[158] Under these rules, the government is privy to information compiled "[a]ny time you write check [sic], use a credit card, buy something on credit, make department store purchases, surf the Web, use an e-z pass to buy gasoline or pay a toll," because those activities are gathered by commercial database companies, and, under the Ashcroft Guidelines, those databases could be subject to government inspection.[159] In addition to being able to acquire profiles of U.S. persons, the FBI gained authority to store this information for future investigatory purposes indefinitely.[160] This raises concerns because data mining services often have inaccurate data from which the FBI can draw inaccurate conclusions[161] and also because some data mining services profile people by race and religion, a feature which could lend itself to systematic racial and religious profiling by the FBI.[162]

Third, the Ashcroft Guidelines doubled the period for the initial authorization to conduct investigations from ninety to 180 days, allowed Special Agents in Charge, instead of FBI Headquarters, to grant the first two extensions of time for preliminary inquiries, and lengthened the duration of these extensions from thirty to ninety days.[163] These changes were described by the ACLU as "open

158. ASHCROFT GUIDELINES, *supra* note 140, at 21.

159. ASHCROFT GUIDELINES, *supra* note 140, at 21; Memorandum from Marvin J. Johnson, *supra* note 140.

160. ASHCROFT GUIDELINES, *supra* note 140, at 21. Though the Privacy Act of 1974 limits the time for which government agencies can keep documents, it also contains very large exceptions. The Act's "General Exemptions" provision, for example, includes "information compiled for the purpose of a criminal investigation." 5 U.S.C. § 552a(j)(2)(B) (2006).

161. The Privacy Act also provides a mechanism through which individuals can correct inaccurate information, but, again, the FBI's data is likely exempted from those requirements. 5 U.S.C. § 552a(d); *see also* Anya Bernstein, *The Hidden Costs of Terrorist Watch Lists*, 61 BUFF. L. REV. 461, 467-68 (2013).

162. *See, e.g.*, Spencer Ackerman, *FBI Crime Maps Now 'Pinpoint' Average Muslims*, WIRED: DANGER ROOM BLOG (Oct. 24, 2011, 1:30 PM), http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims (reporting that "the FBI compiles maps of businesses, community centers and religious institutions in ethnic enclaves around the United States," and specifically in Muslim neighborhoods, with no connection to the investigation of suspected criminal activity); *see also Mapping the FBI: Uncovering Abusive Surveillance and Racial Profiling*, ACLU, http://www.aclu.org/mapping-fbi-uncovering-abusive-surveillance-and-racial-profiling (last visited Mar. 14, 2014).

163. ASHCROFT GUIDELINES, *supra* note 140, at 8-9; *see also* OIG INVESTIGATION, *supra* note 100, at 171.

invitations for fishing expeditions" that would allow the FBI to "spy on citizens and noncitizens, and gather political intelligence for up to one year with no oversight from FBI Headquarters."[164]

Fourth, information gathered during a preliminary inquiry was to be maintained in a database in order to facilitate "the prompt retrieval of information concerning the status (open or closed) and subjects of all such inquiries and investigations."[165] Such a decision raises due process concerns arising from the placement of individuals within a government database without their knowledge and without verification of the facts contained therein.[166] Additionally, the aggregation of highly personal and identifying information into one central database becomes a "honeypot" for hackers and criminals.[167] Finally, and more to the core of the problem, a government database on American activity creates distrust between law enforcement officials and the public, threatening the very safety that the FBI is charged with preserving.[168]

The final significant update occurred with the 2008 Mukasey Guidelines, which, as discussed earlier, created an "Assessment" level of investigation. The Assessment category granted FBI agents a vast amount of investigatory authority premised on no factual evidence whatsoever.[169] Conducting an Assessment allowed FBI agents to:

---

164. Memorandum from Marvin J. Johnson, *supra* note 140; *see also* ASHCROFT GUIDELINES, *supra* note 140, at 21.

165. ASHCROFT GUIDELINES, *supra* note 140, at 21.

166. *See, e.g.*, Bernstein, *supra* note 161, at 462; Peter M. Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804, 837-54 (2007).

167. *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 392.

168. *See, e.g.*, Hubert Williams, Police Found., *Foreword* to ANITA KHASHU, POLICE FOUND., THE ROLE OF LOCAL POLICE: STRIKING A BALANCE BETWEEN IMMIGRATION ENFORCEMENT AND CIVIL LIBERTIES, at vii-viii (2009), *available at* http://www.policefoundation.org/sites/g/files/g798246/f/Khashu%20%282009%29% 20-%20The%20Role%20of%20Local%20Police.pdf.

169. MUKASEY GUIDELINES, *supra* note 132, at 19-20; *see also* Charlie Savage, *Wider Authority for F.B.I. Agents Stirs Concern*, N.Y. TIMES, Oct. 29, 2009, at A1, *available at* http://www.nytimes.com/2009/10/29/us/29manual.html ("The manual authorizes agents to open an 'assessment' to 'proactively' seek information about whether people or organizations are involved in national security threats. Agents may begin such assessments against a target without a particular factual justification. The basis for such an inquiry 'cannot be arbitrary or groundless speculation,' the manual says, but the standard is 'difficult to define.'" (quoting FBI, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE 39-40 (2008) [hereinafter 2008

a. Obtain publicly available information.

b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.

c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.

d. Use online services and resources (whether nonprofit or commercial).

e. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

f. Interview or request information from members of the public and private entities.

g. Accept information voluntarily provided by governmental or private entities.

h. Engage in observation or surveillance not requiring a court order.

i. [Obtain] [g]rand jury subpoenas for telephone or electronic mail subscriber information.[170]

Interestingly, the Assessment level of investigatory authority was adopted from an earlier set of guidelines that governed *foreign* intelligence collection, illustrating how the comparatively lower standards that govern foreign intelligence gathering are being imported and applied to domestic intelligence gathering.[171]

As this Section illustrates, to meet the expanding mission of the FBI, the Attorney General Guidelines expanded the investigatory tools available to the FBI, often in questionable ways. In particular, evolution of the Guidelines shifted the balance originally struck between civil liberties and national security interests by allowing more incursions on rights with comparably fewer facts supporting a national security need.

DIOG], *available at* http://graphics8.nytimes.com/packages/images/nytint/docs/the-new-operations-manual-from-the-f-b-i/original.pdf)).

170. MUKASEY GUIDELINES, *supra* note 132, at 20. This creates the layered approach to creating legitimacy in law. Currently, ECPA allows this and it has come under fire. By creating a provision reemphasizing this authority, the FBI further lends legitimacy to an authority that was previously seen as anomalous and controversial.

171. JOHN ASHCROFT, OFFICE OF THE ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION 19-23 (2003), *available at* http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf.

C. The Recreation of an Intelligence-Gathering Process Cloaked in Secrecy

The third hallmark of the Hoover FBI was secrecy, and we are now experiencing a similar veil of secrecy over the government's domestic intelligence program.

The Attorney General Guidelines are developed behind closed doors, without consulting Congress or the public. Recently, it has been discovered that the FBI, also without consultation with Congress or the public, develops and issues a dense internal manual called the Domestic Investigation and Operations Guide (DIOG), which, by one account "supposedly narrows but in fact expands the Attorney General Guidelines."[172] The DIOG is, as the FBI openly states, a "policy document"[173] in which the Bureau "implement[s]" the Attorney General Guidelines on its own accord, without any formal oversight.[174] In this way, the DIOG is a playbook for the FBI, by the FBI. The FBI found itself in hot water as a result of the 2008 iteration of the DIOG because it authorized a program of "race-and-ethnicity-based profiling."[175] Specifically, the DIOG authorized FBI agents

> to collect and analyze racial and ethnic demographic information to identify and "Geo-map" concentrated ethnic communities and the location of ethnic oriented businesses and facilities "if these locations will reasonably aid in the analysis of potential threats and vulnerabilities" and assist in "intelligence analysis." The DIOG also allows the FBI to collect and track "specific and relevant ethnic behavior" and "behavioral

172. Telephone Interview with Michael German, ACLU Policy Counsel & Former FBI Agent (Feb. 12, 2013).

173. FBI, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE 1-1 (2011), *available at* http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version/fbi-domestic-investigations-and-operations-guide-diog-october-15-2011-part-01-of-03/at_download/file.

174. *FBI Domestic Investigations and Operations Guide (DIOG)*, FBI, http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 (last visited Mar. 14, 2014). The first DIOG was issued on December 16, 2008, and an updated version was issued on October 15, 2011. *Id.* For a copy of the 2008 document, see 2008 DIOG, *supra* note 169.

175. Letter from Laura W. Murphy, Dir., ACLU, to Eric H. Holder, Jr., Att'y Gen. of the U.S. 3 (Oct. 20, 2011), *available at* http://www.aclu.org/files/assets/aclu_letter_to_ag_re_rm_102011_0.pdf.

> characteristics reasonably associated with a particular criminal or terrorist element of an ethnic community."[176]

Perhaps more astounding than the program, is the fact that, though it was authorized in 2008, it was not discovered until 2011.[177] And even then, it was only discovered thanks to the diligent efforts of the advocacy organizations that litigated to learn of both the existence and the facts of the program.[178]

Furthermore, the DIOG has created an unprecedented new level of investigative authority, the "pre-assessment" investigation authority, which allows agents to conduct certain investigations without making any record of it. Despite a recent report that showed that the FBI conducted 82,325 assessments on individuals and groups from March 2009 to March 2011,[179] FBI General Counsel, Valerie Caproni, said that it was "too cumbersome to require agents to open formal inquiries before running quick checks."[180] As a result, the FBI relaxed requirements on conducting investigations by removing the requirement of even needing to *open* an assessment before searching for information about a person in a commercial or law enforcement database.[181] Under the new rules, "agents will be allowed to search such databases without making a record about their decision," thus leaving no paper trail and making it even harder to track and account for government intelligence gathering of Americans.[182]

From the moment the Levi Guidelines were issued, the historical account provided above demonstrates how the DOJ began the slow process of reversion back to old habits. As our collective attention to surveillance and intelligence gathering began to fade, the DOJ was caught in a period of "drift"—a time where it slowly retreated back to old positions. This points to a weakness of administrative constitutionalism: when people are no longer laser focused on redefining the abstract moral language of our

176. *Id.* (quoting 2008 DIOG, *supra* note 169, at 32-33).
177. *Id.*
178. *Id.* at 4.
179. Charlie Savage, *F.B.I. Focusing on Security over Ordinary Crime*, N.Y. TIMES, Aug. 24, 2011, at A16, *available at* http://www.nytimes.com/2011/08/24/us/24fbi.html.
180. Charlie Savage, *F.B.I. Agents Get Leeway to Push Privacy Bounds*, N.Y. TIMES, June 13, 2011, at A1, *available at* http://www.nytimes.com/2011/06/13/us/13fbi.html.
181. *Id.*
182. *Id.*

Constitution, agencies can enter a quiet, solitary process of shadow administrative constitutionalism.

The Attorney General Guidelines were originally drafted to articulate and implement the tentative consensus that emerged from a national dialogue. In this way, the 1976 iteration of the Guidelines demonstrated administrative constitutionalism at work. However, instead of iterating those norms through a robust interbranch, intrabranch, and public dialogue, the Guidelines were iterated internally, drawing inspiration from the isolated echo chambers of the DOJ itself. Over time, the evolution of the norms espoused by the Guidelines shifted the balance between individual rights and national security. Those norms soon became entrenched, without undergoing the deliberation that is assumed within administrative constitutionalism. This evolution reflects shadow administrative constitutionalism at work.

As this Part demonstrates, in the midst of a national conversation, administrative agencies can be valuable vehicles for articulating, implementing, and refining the emerging national consensus. However, when the conversation comes to an end, agencies may continue to develop norms with no anchor in public discourse and no promise of public deliberation. Parts III and IV take a step back to explore why the Attorney General Guidelines evolved the way they did.

III. Norm Entrepreneurship in the Shadows: The Natural Impulse Towards Mission Creep

Why is it that the evolution of the Attorney General Guidelines systematically promoted norms that prioritized national security over civil liberties and expanded the FBI's authority? In this Part, I argue that this phenomenon is the result of the agency's natural impulse towards mission creep. This instinct is a function of two separate conditions both operating in the national security arena: a powerful and loosely defined mandate—preserving our national security—and the medieval structure of bureaucracy. These factors encouraged the creation of policies that rejiggered the balance between civil rights and national security needs in favor of national security.

A. Powerful, Loosely Defined Mandate

The mission of national security is at once so powerful and so vague that mission creep towards complete surveillance is only

natural. After all, it is a Hobbesian reminder of the primary purpose of the state. The state exists to keep us safe from each other and from outsiders. If the citizenry cannot rest assured that their possessions, livelihoods, and lives are stable and secure, then the state has failed in its most fundamental duty. At the highest level, this mandate contains no limiting principles, and the determination of when our national security is threatened is solely in the hands of the executive charged with delivering on the mandate. Thus, while we may negotiate peacetime limitations on the authorities of law enforcement and intelligence gathering, when the security of the nation is called into question, those limitations are easily shrugged off and the mission expanded.

As existential threats to our national security increasingly become a way of life, the FBI is instinctively responding by expanding its mission and pursuing its mission more comprehensively. As Professor Peter Swire explains:

> [A] more general reason why surveillance powers expand over time [is that] intelligence agencies get part of a picture but are unable to understand the entire picture and thus seek and receive additional powers, with the hopes that the additional surveillance capabilities will be more effective at meeting the goal of preventing harm before it occurs.[183]

Thus it is in part the noble pursuit of a powerful but amorphous mandate that motivates mission creep.

The powerful and loosely defined mission also encourages mission creep in an attempt to avoid the public inquiry and blame game that often occur in the wake of an attack. Consider the response to the Boston Marathon bombing in 2013. The FBI was widely blamed for not keeping better tabs on one of the accused bombers, Tamerlan Tsarnaev, a legal, permanent resident of the United States. In early 2011, the FBI received a tip from the Russian government that Tsarnaev was growing increasingly radicalized in his practice of Islam.[184] In response, the FBI "checked U.S. government databases and other information to look for such things as derogatory telephone communications, possible use of online sites associated with the promotion of radical activity, associations with other persons of

183. Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1349 (2004); *see also* David S. Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SECURITY L. & POL'Y 1, 9 (2011).

184. Scott Shane & Michael S. Schmidt, *F.B.I. Did Not Tell Police in Boston of Russian Tip*, N.Y. TIMES (May 10, 2013), http://www.nytimes.com/2013/05/10/us/boston-police-werent-told-fbi-got-warning-on-tsarnaev.html.

interest, travel history and plans, and education history," in addition to interviewing Tsarnaev's family members.[185] The investigation produced little actionable evidence. The FBI shared the information with Russian authorities and asked for additional information on Tsarnaev that might justify further investigation, but did not receive any information.[186]

Despite the fact that the FBI followed protocol, the public and the press fixated on the fact that the FBI was aware of Tsarnaev's radicalization and yet did not prevent the attack in Boston.[187] The public's fear that the attacks represented a failure of the FBI was not allayed by the President's assurances that the FBI managed the situation with the utmost competence, both pre- and post-attack.[188] In a moment of fear, the public demanded 100% prevention, ignoring the fact that perfect prevention is difficult in a society that also protects civil liberties.[189]

This post-attack blame game forces the Justice Department and the FBI to make a difficult decision: Do they aggressively and potentially unconstitutionally expand their vague mandate to include the prevention of all instances of terrorism-related violence, or do they maintain a conservative interpretation of their authority and risk exposing the agency to intense public scrutiny and potentially having the agency brass raked over the coals, regardless of whether or not the FBI or any other element of DOJ was at fault? A reasonable agency head would choose to expand the mandate. After all, as I discuss more fully in Parts IV and V, given the secrecy in which national security policy is made and the sparse oversight to which it is subject, the minimal chance of any exposure of inappropriate or illegal practices is outweighed by the benefits of expanding the mandate.

---

185. Press Release, FBI Nat'l Press Office, 2011 Request for Information on Tamerlan Tsarnaev from Foreign Government (Apr. 19, 2013), *available at* http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government.

186. *Id.*

187. Shane & Schmidt, *supra* note 184.

188. *See id.*

189. This obsession with terrorism prevention exists despite the fact that incidents of domestic terrorism are lower today than they were before 9/11. As recently reported by Elizabeth Goitein and Faiza Patel, "In the 1970s, for example, the U.S. saw an average of 60 to 70 terrorist incidents a year, which is 15 to 20 times higher than the level of terrorist activity seen in most years since 9/11." Elizabeth Goitein & Faiza Patel, *Rethinking the War on Terror*, BOS. REV. (May 28, 2013), http://bostonreview.net/us/rethinking-war-terror.

Given the powerful and loosely defined national security mandate, it is only natural that the FBI's mission creeps from investigating crimes to preventing crime. This expansive interpretation of the mandate encourages aggressive surveillance norms. In this way, the FBI's instinctive promotion of surveillance norms is inevitable.

B. Medieval Structure of Bureaucracy

The proclivity toward mission creep is compounded by a general bureaucratic inclination towards mission creep. Bureaucracies tend to operate as fiefdoms—collecting and holding onto as much power as possible, limiting external oversight of their work, and allowing it only *ex post*.[190] Some scholars, including Daryl Levinson, have questioned this theory, arguing that the "bureaucrats' commitment to a particular mission, or to a particular vision of how that mission ought to be accomplished, might cause them to resist any expansion of agency activity outside of these boundaries."[191] Levinson further argues that agency heads are "high-level political appointees who will be much less invested in the agency's mission and much more interested in pleasing their political overseers"—individuals who likely have no reason to prioritize the expansion of bureaucracy.[192] Such arguments underestimate the natural instincts of individuals to believe that what they are doing is good and useful and therefore that doing more of it is likely better. Furthermore, such arguments assume that agency officials are so politically tied to their "overseers" that they will abandon any desire to create a separate professional legacy of their own.

Together, the nature of bureaucracy and the powerful and loosely defined national security mandate provide one rationale for the evolution of the norms embedded within the Attorney General Guidelines. The next Part of this Article attempts to unpack the conditions that support the entrenchment of those norms into our culture.

---

190. *See, e.g.*, Bruce Ackerman, *The New Separation of Powers*, 113 HARV. L. REV. 633, 700, 703 (2000) (describing the politicized bureaucracy as an "unruly . . . fiefdom[]"). *See generally* WILLIAM A. NISKANEN, JR., BUREAUCRACY AND REPRESENTATIVE GOVERNMENT (1971); JAMES Q. WILSON, BUREAUCRACY: WHAT GOVERNMENT AGENCIES DO AND WHY THEY DO IT (1989).

191. Daryl J. Levinson, *Empire-Building Government in Constitutional Law*, 118 HARV. L. REV. 915, 933 (2005).

192. *Id.*

IV. NORM ENTRENCHMENT IN THE SHADOWS: THE UNWITTING ACCEPTANCE OF AGENCY NORMS INTO CULTURE AND LAW

Norms are traditionally studied in legal scholarship to the extent that they "control individual behavior to the exclusion of law," interact with the law such that they "together influence behavior," influence the development of law, or reflect the influence of law.[193] This Article provides an account of the way in which an administrative agency, through what has been termed "soft law,"[194] is able to influence cultural norms on a given issue, which over time influences the development of hard law in the area. Alternately stated, this Article offers one "theory of origin" for our current pro-surveillance norms and laws in an effort to "help identify the conditions under which . . . [these] norms are likely to arise, conditions which may signal the need for legal intervention."[195]

It is understood that laws can shape societal norms.[196] As McAdams describes, "Various scholars claim that legally restricting

193. *See* McAdams, *supra* note 11, at 347.

194. Jacob Gersen and Eric Posner have described "soft law" as those "statements by lawmaking authorities that do not have the force of law (most often because they do not comply with relevant formalities or for other reasons are not regarded as legally binding), but nonetheless affect the behavior of others." Jacob E. Gersen & Eric A. Posner, *Soft Law: Lessons from Congressional Practice*, 61 STAN. L. REV. 573, 577 (2008) (footnote omitted). While defined broadly, soft law is traditionally studied more narrowly in the context of regulators coercing regulated entities by publicly signaling a threat or promise of tougher or more rigid regulations if certain behaviors are not "voluntarily" adopted. *See, e.g.*, David Zaring, *Best Practices*, 81 N.Y.U. L. REV. 294, 297 (2006) (detailing agencies' use of the "best practices" model of regulation in which "regulated entities themselves devise practices to comply with relatively unspecific regulatory requirements. These practices are selected and publicized as 'best,' but not mandated by central administrators as they would be in regulation through a more traditional vertical command-and-control model. The idea is that these best practices will subsequently be adopted by other regulated entities"). This Article discusses a variant of this traditional notion of soft law. In particular, the focus here is on an agency exercising soft law not to coerce certain behaviors, but instead, to pressure test certain ideas with the public and in some cases, perhaps, to introduce and acclimatize the public to a new norm. Upon the successful socialization of a new "norm," so marked by the general public acceptance of it, the path is now clear for a hard law to be passed if deemed necessary or so desired.

195. McAdams, *supra* note 11, at 391.

196. *See, e.g.*, McAdams, *supra* note 11, at 349; Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 968-72, 1019-25 (1995); *see also* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 905-07 (1996) (using norms to explain changes in smoking behavior, recycling patterns, and gender roles in America).

public smoking may strengthen an antismoking norm, that Title VII impedes enforcement of undesirable norms of race discrimination, and that bans on dueling worked to end norms obligating the duel."[197] Using the same logic, it is no surprise that soft law can also contribute to the way in which societal norms develop.

However, there are certain dangers with the use of soft law. Soft law is developed through a more implicit process, and therefore, lacks the democratic features that are hallmarks of the "hard law" process. As Gersen and Posner explain, "A central tenet of the rule of law is that law be public, so that people may debate it, object to it, and plan their lives around it. Secret law is an anathema and perhaps soft law resembles secret law."[198] Without discounting the utility of soft law in certain circumstances, this Part argues that soft law can have dangerous repercussions when it is used to identify something as complex and core to our democracy as the appropriate balance between privacy and national security because of the impact it allows the government to have on our cultural norms.[199]

As Eskridge and Ferejohn note, the legitimacy of administrative constitutionalism is based on the expectation that

> entrenchment involves public deliberation, . . . the deliberation involves several institutions cooperating together as well as protecting their own authority[,] . . . entrenching deliberation occurs over a long period of time, and the norm does not stick in our public culture until former opponents agree that the norm is a good one (or at least an acceptable idea).[200]

However, as this Part argues, norm entrepreneurship by administrative agencies can result in norm entrenchment even if the intervening deliberation does not occur through the process of shadow administrative constitutionalism. In this Part, I explore this alternate process of norm entrenchment and its implications on culture and law.

---

197. McAdams, *supra* note 11, at 349 (footnotes omitted).

198. Gersen & Posner, *supra* note 194, at 597.

199. By comparison, the use of soft law to identify "best practices for protection and security of 'high-value installations' such as airports, harbors, nuclear power facilities, and military bases[,] . . . best practices in getting Hispanics to wear seat belts," or best practices for "designing workplace policies that would allow disabled individuals to telecommute most effectively" seem inherently less problematic. For these examples and others, see Zaring, *supra* note 194, at 296-97.

200. ESKRIDGE & FEREJOHN, *supra* note 9, at 7.

A. How Entrenchment Happens

In shadow administrative constitutionalism, norm entrenchment is the product of the public's tacit acceptance of bureaucratic policymaking as wise or at least intractable. It is norm entrenchment motivated by path dependency[201] and legitimated by historical practice.

Path dependency reflects an understanding of the relative cost associated with changing course.[202] As President Obama realized in his first term, change requires much more than the support of the electorate.[203] It also requires political will and political capital.[204] Path dependency captures the instincts of government officials to opt for the path of least resistance—to pick their political battles wisely.

Even if the spirit of Edward Levi suddenly overtook the DOJ, the battle to reverse course would be a difficult one. As a first-order matter, changing course implies that the existing course is incorrect—an admission of failure that might expose the agency to unwanted scrutiny and negatively implicate the agency's top brass. Secondly, political support on this issue is not evenly distributed. Though the agency could rely on underrepresented and underfunded activist groups to support a reversion to the previous surveillance norms, the agency would be wise to expect opposition from the powerful defense contractor lobby and the national security war hawks that would argue that the country's security was compromised as a consequence.

---

201. For a broader discussion of path dependency in law and politics, see generally Oona A. Hathaway, *Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System*, 86 IOWA L. REV. 601 (2001); Paul Pierson, *Increasing Returns, Path Dependence, and the Study of Politics*, 94 AM. POL. SCI. REV. 251 (2000); Richard A. Posner, *Past-Dependency, Pragmatism, and Critique of History in Adjudication and Legal Scholarship*, 67 U. CHI. L. REV. 573 (2000).

202. *See* Aziz Z. Huq, *Structural Constitutionalism as Counterterrorism*, 100 CALIF. L. REV. 887, 908 (2012) ("[A]s an agency invests in expertise and turf battles, it becomes more set in its ways and hence more reluctant to reorient toward new problems and to respond to new policy challenges.").

203. *See* Matt Viser, *Still Talking About Change in a Time of Broken Politics*, BOS. GLOBE, Jan. 20, 2013, at A1, *available at* http://www.bostonglobe.com/news/politics/2013/01/20/president-obama-will-use-first-term-lessons-and-campaign-tactics-tackle-challenges-next-four-years/zjys4IsoEhJH9gbTtS2AFP/story.html (citing Obama's official Jim Messina as stating, "'One thing we learned in the first term, especially the first two years, was it became a very inside Washington game to pass these things'").

204. *See id.*

The second mechanism that creates entrenchment is historical practice. Over time, the norms adopted through path dependency become accepted as correct. A given historical practice gains legitimacy under the belief that what is time-tested is true. However, such a belief assumes that time has offered its fair share of critics and that only those things that are sturdy enough to withstand the assault of those critics earn the title of "time-tested and true." The evolution of the Guidelines can be understood to demonstrate that such an assumption is not always deserved. Rather, the Guidelines show us that entrenchment can simply be the product of slow movements in one direction building upon each other, each additional movement unfairly affirming the directional accuracy of the one before it. By the time we are miles to the right of where we started, we feel as if this new place is correct simply because, if it were not, surely someone would have stopped us earlier. Thus, norm entrenchment that results from historical practice assumes deliberation or, at the very least, assumes our implicit collective consent to the norm itself, evidenced, circularly, by the continued operation of the norm.

Putting it all together, the norm entrepreneurship that began after the passage of the Levi Guidelines combined with the proclivity towards path-dependency created a one-way ratchet for surveillance authority, where the size of each shift was a factor of the priorities and temperament of the President, his Attorney General, and his FBI Director. The norms introduced are ultimately deemed appropriate by virtue of the wisdom of historical practice. The next Section discusses the implication of the entrenchment of these surveillance norms.

B. Surveillance Culture

Under this theory of shadow administrative constitutionalism, over time, an agency can, unwittingly, influence and shift our collective sense of normal. The balance between free speech and national security was quietly but progressively shifted through the various iterations of the Attorney General Guidelines. Without public awareness, let alone public deliberation, the new balance has become one that we have come to accept as correct. That surveillance is increasingly commonplace today and that people understand this not as a violation of their rights but as a small price to pay for security—this is the consequence of shadow administrative constitutionalism.

Consider FISA. The basic structure of FISA remained unchanged from 1978 until September 11, 2001.[205] In response to 9/11, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001 (the PATRIOT Act), which revised FISA to make it easier to gather intelligence information, despite the impact that that easing had on Americans' civil liberties.[206]

The PATRIOT Act tore down the "wall" separating foreign intelligence activities from domestic law enforcement,[207] created authority for a roving wiretap,[208] and authorized more expansive access to private business records.[209] The changes resulting from the PATRIOT Act were immediately felt. "In 2003, for the first time, the number of surveillance orders issued under FISA exceeded the number of law enforcement wiretaps issued nationwide."[210]

Because the PATRIOT Act was rushed through Congress in what was a state of emergency, many of the Act's more aggressive provisions, including the FISA provisions, were scheduled to sunset on December 31, 2005.[211] However, when the time came for sunset, after significant debate, the PATRIOT Act was renewed.[212] Reflecting the high tensions during the debate, "[s]ome lawmakers who voted for the bill expressed deep reservations about it, and the Republican chairman of the Senate Judiciary Committee [had] already [begun] drafting further legislation to revise it."[213] Tensions ultimately subsided, however, and no such legislation was passed. Instead, in 2008, a new law, the FISA Amendments Act, was passed

---

205. Swire, *supra* note 183, at 1308.

206. Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of the U.S. Code).

207. *See* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2006); *see also* Swire, *supra* note 183, at 1308.

208. *See* 50 U.S.C. § 1805(c)(2)(B).

209. *See id.* § 1861.

210. *See* Swire, *supra* note 183, at 1308.

211. CHARLES DOYLE, CONG. RESEARCH SERV., RL32186, USA PATRIOT ACT SUNSET: PROVISIONS THAT EXPIRE ON DECEMBER 31, 2005, at 2 (2005), *available at* https://www.fas.org/sgp/crs/intel/RL32186.pdf.

212. *Permanent Provisions of the Patriot Act: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 1-2 (2011) (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism & Homeland Sec.).

213. *See* Sheryl Gay Stolberg, *Senate Passes Legislation to Renew Patriot Act*, N.Y. TIMES, Mar. 3, 2006, at A14, *available at* http://www.nytimes.com/2006/03/03/politics/03patriot.html?_r=0.

to further expand the FBI's authority on matters of surveillance.[214] And since 2009, despite the election of a President who pledged to correct the previous Administration's abuse of executive power, expiring provisions of FISA have been reauthorized every year, amid significantly less fanfare than the first debate in 2005.[215] The latest round of FISA extensions was quietly passed at the end of 2012, the day before the amendments were set to expire, under the din of the fiscal cliff debates.[216]

The amendments made to FISA since 9/11 reflect the public's growing acceptance of broader government encroachment on civil liberties through massive, unregulated surveillance. For example, in June 2013, immediately after *The Guardian* and *The Washington Post* exposed massive, dragnet NSA surveillance programs implicating significant amounts of domestic communication, a Pew Research Center poll indicated that Americans were *less* concerned about NSA spying than they were in 2006 in the wake of the Bush Administration's warrantless wiretapping program.[217] The poll found that

> [o]verall, 56 percent of Americans consider the NSA's accessing of telephone call records of millions of Americans through secret court orders "acceptable," while 41 percent call the practice "unacceptable." In 2006, when news broke of the NSA's monitoring of telephone and e-mail

214. *See* Eric Lichtblau, *Deal Is Struck to Overhaul Wiretap Law*, N.Y. TIMES, June 20, 2008, at A1, *available at* http://www.nytimes.com/2008/06/20/washington/20fisacnd.html (discussing the creation of Section 702 and other expansions of FISA authority).

215. EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 1 (2013), *available at* http://www.fas.org/sgp/crs/intel/R42725.pdf.

216. *Id.*; *see also* Bill Keller, Op-Ed., *Invasion of the Data Snatchers*, N.Y. TIMES, Jan. 14, 2013, at A23, *available at* http://www.nytimes.com/2013/01/14/opinion/keller-invasion-of-the-data-snatchers.html ("Likewise, while we were all distracted by the dance on the fiscal cliff, the 112th Congress in its final days whisked through a renewal of the law that governs eavesdropping by American intelligence agencies on Americans' phone calls and e-mail traffic. A couple of senators made modest attempts to hold the eavesdroppers more accountable by, for example, disclosing the number of law-abiding citizens whose communications have been intercepted. Their efforts were voted down.").

217. Jon Cohen, *Most Americans Back NSA Tracking Phone Records, Prioritize Probes over Privacy*, WASH. POST (June 10, 2013), http://www.washingtonpost.com/politics/most-americans-support-nsa-tracking-phone-records-prioritize-investigations-over-privacy/2013/06/10/51e721d6-d204-11e2-9f1a-1a7cdee20287_story.html; *see also* Greenwald, MacAskill & Poitras, *supra* note 2.

> communications without court approval, there was a closer divide on the practice—51 percent to 47 percent.[218]

While there is a significant difference between the two scenarios—in 2006, the surveillance was conducted without any judicial oversight, whereas the more recent instance involves court orders of some variety (secret ones, from a secret court)—the poll speaks to a broader acceptance of surveillance as a practice. This acceptance is the product of and further encourages the seeming ubiquity of authorized surveillance. It is a virtuous or a vicious cycle, depending on your point of view. The continued existence of surveillance makes us more comfortable with it, and our increased comfort can be read as tacit acceptance of surveillance as a feature of daily life.

And the incursion into individual privacy only grows deeper every day. On July 9, 2012, *The New York Times* reported that "cellphone carriers reported that they responded to a startling 1.3 million demands for subscriber information last year from law enforcement agencies seeking text messages, caller locations and other information in the course of investigations."[219] Furthermore, the number of government requests for consumer information from private companies are growing.[220] *The Times* reported that law-enforcement requests writ large have been growing "with annual increases of between 12 percent and 16 percent in the last five years."[221]

In fact, the U.S. has become the global leader in these sorts of requests. Twitter released a report indicating that, between January 1 and June 30 of 2012, it received 849 government requests for user information globally, 679 of which came from the United States.[222] In that same time period, the United States government also led the

---

218. Cohen, *supra* note 217.

219. Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1, *available at* http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html.

220. *See id.* at A9.

221. *Id.*

222. *Information Requests: January 1–June 30, 2012*, TWITTER, https://transparency.twitter.com/information-requests/2012/jan-jun (last visited Mar. 14, 2014).

world in individual requests for user data made to Google at 7,969, requesting information on a total of 16,281 accounts.[223]

As one intelligence official stated, the theory under which four-star general and former Director of the NSA, Keith Alexander, traditionally operated was one that said, "'Rather than look for a single needle in the haystack, . . . [l]et's collect the whole haystack.'"[224] By having the ability to "'[c]ollect it all, tag it, store it,'" the NSA would be able to go sifting through the data dump whenever it needed to.[225]

Responding to current surveillance norms, the government is seeking to codify new mechanisms for intelligence gathering. In July 2012, the White House came out in support of the Lieberman-Collins Bill, a cybersecurity measure that would allow unprecedented amounts of information sharing between private companies, collecting terabits of data on consumers, and the government.[226] The information sharing provisions of the Lieberman-Collins Bill allow for the unencumbered exchange of vaguely defined "cybersecurity threat indicators" between private entities and, furthermore, allow private entities designated as "cybersecurity exchanges" to disclose cybersecurity threat information to the government.[227] To encourage participation in the data-sharing program, private entities are promised full immunity for any consumer lawsuits arising from their participation.[228] While the Lieberman-Collins Bill failed to make it

---

223. *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2012-06 (last visited Mar. 14, 2014).

224. Ellen Nakashima & Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All,' Observers Say*, WASH. POST, July 14, 2013, http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

225. *Id.*

226. EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATIVE POLICY: S. 3414—CYBER SECURITY ACT OF 2012 (2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saps3414s_20120726.pdf; Jennifer Granick, *Revised Cybersecurity Act Needs Amendments for Privacy, Security*, CENTER FOR INTERNET & SOC'Y (July 20, 2012, 4:58 PM), http://cyberlaw.stanford.edu/blog/2012/07/revised-cybersecurity-act-needs-amendments-privacy-security.

227. Cybersecurity Act of 2012, S. 2105, 112th Cong. §§ 701-08 (2012) (authorizing "any private entity [to] disclose lawfully obtained cybersecurity threat indicators to any other private entity" and to federally operated "cybersecurity exchanges").

228. *See id.* § 706(a)(2)(D).

out of committee,[229] similar language was passed by the House of Representatives in its Cyber Intelligence Sharing and Protection Act (CISPA) by a vote of 288 to 127.[230] The introduction and passage of such bills in the House of Representatives emphasizes the new normal in surveillance culture: the government gathers the haystack without probable cause and searches for the needle—or at least something shiny.

In today's surveillance culture, laws and practices that authorize more and more government spying are permissible, if not expected. As a result, the acceptable boundaries of surveillance law have become so broad that, until recently, the New York Police Department was engaging in a targeted surveillance effort of Muslim student groups "at more than a dozen universities across the Northeast, framing the effort as one way to guard against the threat of terrorism."[231] Former New York City Mayor Michael Bloomberg said of the NYPD's program, "'That's what you would expect them to do. That's what you would want them to.'"[232]

There are some criticisms of this account of surveillance culture. At the highest level, there is the counterargument that our surveillance culture is something that we have willingly agreed to—not something that has been foisted upon us, unwittingly.[233] There are two forms of this counterargument. One argues that surveillance culture is something we understand and accept when we choose

---

229. Jennifer Martinez & Ramsey Cox, *Senate Votes Down Lieberman, Collins Cybersecurity Act a Second Time*, HILL BLOG (Nov. 14, 2012, 11:12 PM), http://thehill.com/blogs/hillicon-valley/technology/268053-senate-rejects-cybersecurity-act-for-second-time.

230. 159 CONG. REC. H2130, H2144 (daily ed. Apr. 18, 2013). CISPA authorizes the sharing of "cyber threat information . . . with the . . . Government" and further allows the government to use that information for any number of purposes, including not only the prevention of cyber-terrorism, but also "the investigation and prosecution of cybersecurity crimes[,] . . . the investigation and prosecution of crimes involving . . . danger of death or serious bodily harm[,] . . .[and] the protection of minors from child pornography." Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. § 2(c)(1) (2013).

231. *See* Al Baker & Kate Taylor, *Mayor Defends Monitoring of Muslim Students on Web*, N.Y. TIMES, Feb. 22, 2012, at A18. This program has recently been shut down. Matt Apuzzo & Joseph Goldstein, *New York Drops Unit That Spied on Muslims*, N.Y. TIMES (Apr. 15, 2014), http://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html.

232. *Id.* (quoting New York City Mayor Michael R. Bloomberg).

233. I thank Professor Molly Land and Dru Brenner-Beck for each separately flagging this point for me.

"free" communication, networking, and entertainment applications in exchange for our privacy. In a world where we agree to allow Google's algorithms to read our emails so that they may direct relevant advertising our way, can we really say that it is the evolution of the Attorney General Guidelines that has made us numb to surveillance? The other form of the argument suggests that the national conversation that occurred after 9/11 affirmed the new national security norms. This was demonstrated by the overwhelming support for the PATRIOT Act both when it was first passed and when its provisions were set to expire.[234]

Both of these arguments are unsatisfying. Taking each in turn, there is no reason to think that because we agree to provide information to Google, we also agree to provide that same information to the government. There is undoubtedly some reduction in privacy that we have all come to accept in this highly data-driven existence we collectively lead, but a reduction in privacy *vis-a-vis* the private companies with which we transact does not necessarily imply a reduced expectation of privacy with the government. This is for obvious reasons. I share information with Google because Google uses that information to show me advertisements I might find useful or make my search queries more personalized. However, sharing information with the government is a different proposition all together. While the government may use my information to more efficiently and effectively deliver services, it can also use my information in more insidious ways. After all, the government is the only institution that can legitimately use force against its citizens. It can preventatively institutionalize dangerous persons,[235] and, perhaps more likely, it can wield the immense power of the administrative state against its citizens, inhibiting their ability to travel (no-fly lists) and making it difficult to obtain social services and benefits.[236] As

234. Thanks to Professor Rob Knowles for this astute insight.

235. Carol S. Steiker, *Foreword: The Limits of the Preventative State*, 88 J. CRIM. L. & CRIMINOLOGY 771, 774 (1998) ("But punishment is not the only, the most common, or the most effective means of crime prevention. The state can also attempt to identify and neutralize dangerous individuals before they commit crimes by restricting their liberty in a variety of ways. In pursuing this goal, the state often will expand the functions of the institutions primarily involved in the criminal justice system—namely, the police and the prison. But other analogous institutions, such [as] the juvenile justice system and the civil commitment process, are also sometimes tools of, to coin another phrase, the 'preventive state.'" (footnote omitted)).

236. Joe Silver, *After Seven Years, Exactly One Person Gets Off the Gov't No-Fly List*, ARSTECHNICA (Mar. 27, 2014, 6:10 PM), http://arstechnica.com/tech-

Professor Jack Balkin has suggested, "Governments will use surveillance, data collection, and data mining technologies not only to keep Americans safe from terrorist attacks but also to prevent ordinary crime and deliver social services."[237]

The alternate argument, that surveillance culture is something that the public has intentionally accepted after 9/11, is also unsatisfying. Consider the evolution of the public response to the 2013 NSA surveillance scandal versus the 2006 NSA surveillance scandal.[238] As I discussed earlier, the first polls that came out after the Snowden leaks indicated that the level of outrage against the 2013 scandal was notably less than the outrage that followed the 2006 scandal.[239] However, importantly, as time went on and more information was released with regards to this latest scandal, the outrage has grown. A 2013 Quinnipiac University Polling Institute poll conducted one month after the Snowden leaks found that 45% of Americans said that government goes too far in restricting civil liberties as part of the war on terrorism, while only 40% said that government does not go far enough to adequately protect the country.[240] The finding contrasted a poll taken in 2010 by Quinnipiac, which showed that only 25% of Americans said government goes too far in restricting civil liberties, while 63% said government does not go far enough.[241]

This poll, when understood in the context of the Pew polling data I discussed earlier, tells an interesting story: immediately after the Snowden leak, the public displayed *more* support for government surveillance practices than it did in the years more immediately following 9/11. However, after more information emerged on the scope of intelligence-gathering activities at issue, that support noticeably dwindled. It can hardly be the case that a culture that truly reflects national consensus shifts upon learning the details of the surveillance programs it supposedly supports. Rather, this polling

---

policy/2014/03/after-seven-years-exactly-one-person-gets-off-the-govt-no-fly-list/ (discussing one woman's "'Kafkaesque' legal battle over the government no-fly list").

237. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 4 (2008).

238. *See supra* text accompanying notes 217-18.

239. *See supra* notes 217-18 and accompanying text.

240. PETER BROWN, QUINNIPIAC UNIV. POLLING INST., U.S. VOTERS SAY SNOWDEN IS WHISTLE-BLOWER, NOT TRAITOR, QUINNIPIAC UNIVERSITY NATIONAL POLL FINDS; BIG SHIFT ON CIVIL LIBERTIES VS. COUNTER-TERRORISM (2013), *available at* http://www.quinnipiac.edu/images/polling/us/us07102013.pdf.

241. *Id.*

data calls into question whether the PATRIOT Act in fact reflected a new national consensus on surveillance norms.

V. CONDITIONS THAT FACILITATE SHADOW ADMINISTRATIVE CONSTITUTIONALISM

Having explored the motivations for norm entrepreneurship and norm entrenchment, this Part explores the conditions that facilitate shadow administrative constitutionalism in the national security arena.[242] In particular, this Part suggests there are two features of national security policymaking that make it a breeding ground for shadow administrative constitutionalism: first, the "super-deference" that applies to agency activity in this area, and second, the secrecy that necessarily accompanies national security policymaking.

A. "Super-Deference"

There is a strong culture of deference to agencies on issues of national security. This is the result of two different cultures of deference at play: the deference that applies to the executive branch's central authority and responsibility to protect our national security, and the deference given to agency expertise as noted in *Holder v. Humanitarian Law Project*.[243] These distinct rationales create a compounding effect that results in what I call "super-deference" to the executive branch on national security issues.[244]

---

242. Though this area is still under-theorized, there has been a flurry of post-9/11 scholarship on the role of administrative agencies in the national security arena. *See, e.g.*, Eric A. Posner & Cass R. Sunstein, Chevron*izing Foreign Relations Law*, 116 YALE L.J. 1170, 1173 (2007); Cass R. Sunstein, *Administrative Law Goes to War*, 118 HARV. L. REV. 2663, 2672 (2005); Adrian Vermeule, *Our Schmittian Administrative Law*, 122 HARV. L. REV. 1095, 1101 (2009); John Yoo, *Administration of War*, 58 DUKE L.J. 2277, 2281 (2009).

243. 130 S. Ct. 2705, 2727 (2010).

244. *Cf.* Sunstein, *supra* note 242, at 2671 ("[T]he President [should] receive[] the kind of super-strong deference that derives from the combination of *Chevron* with what are plausibly taken to be his constitutional responsibilities."). My theory of super-deference is different from Professor Sunstein's "super-strong deference" largely because I am referring to deference to the agency, not the President. *Chevron* deference applies to agencies as understood under the Administrative Procedures Act (APA). *See* 5 U.S.C. § 553 (2012). The President does not fall within the purview of the APA, and therefore does not trigger *Chevron* deference. Instead, the President receives deference in accordance with the *Youngstown* framework, which outside of times of emergency, provides for limited

Alexis de Tocqueville recognized early on in this country's history that "[i]t is chiefly in its foreign relations that the executive power of a nation finds occasion to exert its skill and . . . strength."[245] De Tocqueville presciently noted, "If the existence of the [American] Union were perpetually threatened, . . . the executive . . . would assume . . . increased importance."[246] For the early part of American history, threats to American existence were occasional and short-lived, limiting the growth of executive power.[247] However, the "chronic international crisis known as the Cold War," as Arthur Schlesinger later found, "at last gave presidents the opportunity for sustained exercise of . . . almost royal prerogatives."[248] The executive possessing "almost royal prerogative[]"—what Schlesinger termed the "[i]mperial [p]residency"—reached its apex with President Nixon.[249]

To curb the excesses of executive power, Congress, contemporaneously with the issuance of the Attorney General Guidelines, passed the War Powers Resolution,[250] the National Emergencies Act,[251] the International Emergency Economic Powers Act,[252] and the Inspector General Act of 1978.[253] However, as Professors Eric Posner and Adrian Vermeule argue, these efforts, though well-meaning, were largely ineffective, and the regrowth of

---

deference to the President. *See* Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 635-37 (1952) (Jackson, J., concurring). The *Youngstown* framework highlights a second order point, which is that agency action in the area of national security receives considerable deference as an ordinary matter, whereas presidential decision making in the area of national security receives heightened deference only during time of emergency. *Id.* By this account, administrative constitutionalism allows agencies to shift constitutional norms in a way the President would be unable to unless she was in the midst of a national emergency, where her powers would be at their apex. *Id.*

245. 1 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 158 (Francis Bowen ed., Henry Reeve trans., 6th ed., Boston, John Allyn 1876).

246. *Id.*

247. ARTHUR M. SCHLESINGER, JR., THE IMPERIAL PRESIDENCY, at x (First Mariner Books 2004) (1973).

248. *Id.*

249. *Id.* at x, xvi.

250. War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973) (codified at 50 U.S.C. §§ 1541-48 (2006)).

251. National Emergencies Act, Pub. L. No. 94-412, 90 Stat. 1255 (1976) (codified in scattered sections of 50 U.S.C.).

252. International Emergency Economic Powers Act, Pub. L. No. 95-223, 91 Stat. 1625 (1977) (codified in scattered sections of 50 U.S.C.).

253. Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified at 5 U.S.C. app. 3).

executive power began soon after the dust settled from the tumult of the early 1970s.[254] Key causes for the failed reform effort include a combination of judicial deference to the executive branch on political questions, national security, and foreign affairs efforts, and limited resources for both congressional oversight as well as internal executive branch checks and balances.[255]

Separately, this history reminds us that, unlike other areas in which the executive branch exercises authority, executive expertise on issues of war, peace, and the various states of security that exist in between is authoritative. Agencies acting pursuant to the national security mandate—including the DOJ, the FBI, the CIA, the Department of Defense (DOD), and the National Security Agency (NSA)—are granted deference in their decisions because they are understood to operate with a level of expertise that is unrivaled among the three branches of government. In *Holder v. Humanitarian Law Project*, the Court emphasized the appropriateness of this sort of deference by reiterating a point it had previously made in *Boumediene v. Bush* that "'neither the Members of this Court nor most federal judges begin the day with briefings that may describe new and serious threats to our Nation and its people.'"[256] Consequently, the Court held that "when it comes to collecting evidence and drawing factual inferences" on national security issues, "'the lack of competence on the part of the courts is marked,' and respect for the Government's conclusions is appropriate."[257] Thus, agency norm entrepreneurship on issues of national security will often receive a level of deference that undercuts the deliberative process required under administrative constitutionalism.[258]

Operating together, agency expertise and executive branch authority on national security elicit a sort of super-deference that applies to agency norm entrepreneurship in the national security arena.

---

254. ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 86-87 (2010).

255. *See id.*

256. Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2727 (2010) (quoting Boumediene v. Bush, 553 U.S. 723, 797 (2008)).

257. *Id.* (citation omitted) (quoting Rostker v. Goldberg, 453 U.S. 57, 65 (1981)).

258. *See also* Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 26 (2008) (deferring to the executive branch's reasoning for according weight to national security claims).

B. Secrecy

The second reason national security policymaking lends itself to shadow administrative constitutionalism is secrecy. National security demands the government operate with some secrecy. Announcing our plan of attack or our weakest defenses threatens to sacrifice national security at the altar of transparency. As Former Attorney General Benjamin Civiletti noted in a law review article over thirty years ago:

> Even if we are able to gain information concerning a hostile foreign nation, our success will be shortlived [sic] if we disclose the facts of our success. Further, if we reveal the information obtained, we will not only lose our advantage and risk changes in the acquired plans, but we will also jeopardize or perhaps destroy our sources and methods of gathering information.[259]

With transparency in the national security context at times fundamentally at odds with the mission, the deliberation that is facilitated through open dialogue is significantly hampered.

Comparatively, agencies outside the national security arena are required to be transparent with their findings, their sources of information, and, most of all, their successes and failures. This transparency is built into the notice-and-comment requirements of the Administrative Procedures Act and mandated more generally by the Freedom of Information Act, both of which bind most agencies.[260] However, both statutes provide explicit exemptions for national security purposes.[261] As a consequence, national security policymaking often occurs in secret, avoiding the public deliberation that occurs with more transparent institutions.

---

259. Benjamin R. Civiletti, *Intelligence Gathering and the Law: Conflict or Compatibility?*, 48 FORDHAM L. REV. 883, 888 (1980).

260. Freedom of Information Act, 5 U.S.C. § 552(a) (2012); Administrative Procedures Act, 5 U.S.C. § 553 (2012).

261. The FOIA exemption for national security is codified at 5 U.S.C. § 552(b)(7). Under the APA, agencies can seek a "good cause" exception to the notice-and-comment provisions. 5 U.S.C. § 553(b)(3)(B). As some have mentioned, "[T]he mere mention of national security tends to suggest good cause for immediate government action, even when the government is actually loosening previously established regulations." William S. Jordan, III, *Rulemaking*, *in* DEVELOPMENTS IN ADMINISTRATIVE LAW AND REGULATORY PRACTICE 2011, at 12 (Jeffrey S. Lubbers ed., 2012), *available at* http://www.americanbar.org/content/dam/aba/events/administrative_law/2011/11/2011_fall_administrativelawconference/rulemaking_chapter_2011.authcheckdam.pdf.

VI. FORCING ADMINISTRATIVE CONSTITUTIONALISM OUT OF THE SHADOWS

Administrative constitutionalism can morph into shadow administrative constitutionalism when agency norms are allowed to develop in the shadows and become entrenched without deliberation. To force administrative constitutionalism from the shadows, deliberation-forcing mechanisms must be created and reinforced. Such mechanisms must ensure three types of deliberation: intrabranch, interbranch, and public. This final Part proceeds by first exploring the failure of existing mechanisms of deliberation in the context of the Attorney General Guidelines and then suggesting ways in which to modify or reinforce these mechanisms. Importantly, some suggestions are more viable than others, and I will offer an initial, rough assessment of the viability of each suggestion.

A. Checks and Balances Within the Executive Branch

The growth of executive power and the administrative state has been a fascinating area of scholarship for the last twenty years, with each President providing more intellectual fodder than his predecessor.[262] As one scholar has noted, "While it was relatively rare, and for the most part inconsequential, during the eighteenth and nineteenth centuries, unilateral policy making has become an integral feature of the modern presidency."[263]

---

262. To be fair, the growth of executive power was discussed and documented long before the Clinton Administration. Arthur Schlesinger's book, *The Imperial Presidency*, marks the beginning of the academic focus on executive power. SCHLESINGER, *supra* note 247; *see also* HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR (1990); Steven G. Calabresi & Saikrishna B. Prakash, *The President's Power to Execute the Laws*, 104 YALE L.J. 541 (1994); Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245 (2001); M. Elizabeth Magill, *Beyond Powers and Branches in Separation of Powers Law*, 150 U. PA. L. REV. 603 (2001); Cornelia T.L. Pillard, *The Unfulfilled Promise of the Constitution in Executive Hands*, 103 MICH. L. REV. 676 (2005); Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006); BRUCE ACKERMAN, THE DECLINE AND FALL OF THE AMERICAN REPUBLIC (2010); Trevor W. Morrison, *Constitutional Alarmism*, 124 HARV. L. REV. 1688 (2011) (reviewing ACKERMAN, *supra*).

263. WILLIAM G. HOWELL, POWER WITHOUT PERSUASION: THE POLITICS OF DIRECT PRESIDENTIAL ACTION 179 (2003). For the Clinton Administration, this point is chronicled in Justice Elena Kagan's early piece, *Presidential Administration*. *See* Kagan, *supra* note 262.

To rein in an increasingly powerful executive, some scholars have suggested that the executive branch bureaucracy, comprised of it its many agencies and offices, can provide its own checks and balances.[264] These checks and balances might include some combination of interagency review of national security policies and procedures,[265] direct oversight of national security activities by high-ranking members of the executive branch,[266] and encouragement of dissent and whistleblowing.[267]

1. *Interagency Review*

Interagency review of executive branch action ensures that the often disparately motivated and sometimes diametrically opposed agencies and offices within the executive branch temper the bureaucratic instincts of any one agency or office.

The recent politics around drone warfare provide an illustrative example. Drone strikes, the unmanned aerial attacks that have gained popularity both for their ability to keep U.S. personnel outside of harm's way and for their ability to target suspects with a comparatively high degree of accuracy,[268] have been used by the U.S. government only after the 9/11 attacks and have increased in frequency under the Obama Administration.[269] However, despite

264. Katyal, *supra* note 262.

265. Professor Harold Koh suggested interagency review as a useful check on executive power nearly twenty-five years ago in his book, *The National Security Constitution: Sharing Power After the Iran-Contra Affair*. *See* KOH, *supra* note 262, at 161-62.

266. *See, e.g.*, Katyal, *supra* note 262, at 2324-27; *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 96 (2008) (noting the importance of independent "embedded privacy experts" in the Department of Homeland Security "specifically charged with advancing privacy among competing agency interests, located in a central position within the agency decisionmaking structure, drawing on internal relationships and external sources of power, and able to operate with relative independence").

267. Katyal, *supra* note 262, at 2328-30.

268. *See* President Barack Obama, Remarks at the National Defense University (May 23, 2013), *available at* http://www.npr.org/2013/05/23/186305171/transcript-obama-addresses-counterterrorism-drones.

269. Greg Miller, Ellen Nakashima & Karen DeYoung, *CIA Drone Strikes Will Get Pass in Counterterrorism 'Playbook,' Officials Say*, WASH. POST (Jan. 19, 2013), http://www.washingtonpost.com/world/national-security/cia-drone-strikes-will-get-pass-in-counterterrorism-playbook-officials-say/2013/01/19/ca169a20-618d-11e2-9940-6fc488f3fecd_story_1.html.

their prevalence, the authority and parameters of their use has remained murky.[270]

After receiving considerable public pushback on the legality of the Administration's drone program, the White House began crafting a counterterrorism "playbook" that "establish[ed] clear rules for targeted-killing operations."[271] While the primary goal of the playbook was to transfer drone operations from the opacity of the CIA to the relative transparency of the Defense Department, the playbook also tightened standards by requiring "White House approval of drone strikes and the involvement of multiple agencies—including the State Department—in nominating new names for kill lists."[272] The hope of this latter requirement is that the diplomatic expertise of the State Department and the legal expertise of the DOJ will act as counterweights to the DOD's hawkish instincts, exemplifying how internal checks and balances successfully might rein in executive power.[273]

Comparatively, the Attorney General Guidelines have been issued by the DOJ without any formal interagency review. The Guidelines are not mandatorily shared with any other department or office that might provide a counterweight to the DOJ.[274] However, demanding interagency review begs the question: which agencies would be appropriate reviewers? Which agencies could represent the civil liberties side of the national security debate? There are no obvious candidates.

---

270. This "murkiness" was on full display in the aftermath of the drone strike that killed American citizen and Muslim cleric, Anwar al-Awlaki. Mark Mazzetti, Eric Schmitt & Robert F. Worth, *C.I.A. Strike Kills U.S.-Born Militant in a Car in Yemen*, N.Y. TIMES, Oct. 1, 2011, at A1. Furthermore, despite recent Obama Administration speeches and leaks intended to clarify the U.S. position on drone strikes, there are still more questions than answers. *See* Obama, *supra* note 268.

271. Miller, Nakashima & DeYoung, *supra* note 269.

272. *Id.*

273. *Id.* Interestingly, the playbook makes one large exception: the CIA's drone campaign in Pakistan. *Id.* None of the rules—the transparency, the internal checks and balances—apply to Pakistan. *Id.* This is because senior administration officials "have been reluctant to alter the rules because of the drone campaign's results." *Id.* This further corroborates the view that the strength of the national security mandate makes comprehensive oversight over national security programs and initiatives very difficult. *See id.*

274. The Attorney General obtains authority to issue governing guidelines for the FBI from Executive Order 12,333, which states that the FBI is subject to "the supervision of the Attorney General and [must act] pursuant to such regulations as the Attorney General may establish." *See* 3 C.F.R. § 1.14 (1982).

That is not to say that there have not been efforts to create an agency dedicated to representing civil liberties concerns within the executive branch. *The Final Report of the National Commission on Terrorist Attacks upon the United States* (9/11 Commission) recommended, "[T]here should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."[275] As a result, the Privacy and Civil Liberties Oversight Board (PCLOB) was authorized in 2004.[276] However, the path from authorization to operationalization was a long one. Thanks in part to pressure from a bipartisan group of Senators, the Bush White House finally instituted the Board, and, on March 14, 2006, the PCLOB was finally up and running.[277] By June 2007, the PCLOB had fallen apart with one member resigning because he felt that the organization was not sufficiently independent to effectively do its job.[278] The PCLOB was indeed far from independent. As one report indicates:

> [The PCLOB] was located in the EOP [Executive Office of the President], an enclave of agencies immediately serving the President. Only two of its five members were subject to Senate approval, and all five served at the pleasure of the President. Its advice was to be "to the President or to the head of any department or agency of the executive branch." Although it was to report to Congress at least annually, it was not clear if its members or chair would testify before congressional committees or if the board could otherwise assist Congress. The board's budget was presented as an account within the funding request for the White House Office (WHO), suggesting that it was a subunit of the WHO (although the board's chartering legislation placed it in the EOP, making it a coequal agency to the WHO).[279]

---

275. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 395 (2004) [hereinafter 9/11 COMMISSION REPORT].

276. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1061-62, 118 Stat. 3638, 3684-88 (2004) (codified at 5 U.S.C. § 601 note (2006)).

277. GARRETT HATCH, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS 4 (2012), *available at* https://www.fas.org/sgp/crs/misc/RL34385.pdf.

278. *Id.* at 4-5. Lanny Davis resigned on May 14, 2007 because "he felt the board members had interpreted their oversight responsibilities too narrowly and that they had not exercised adequate independence when they accepted extensive redlining by Administration officials of the board's first report to Congress." *Id.* at 4; *see also* John Solomon & Ellen Nakashima, *White House Edits to Privacy Board's Report Spur Resignation*, WASH. POST, May 15, 2007, at A5.

279. HATCH, *supra* note 277, at 5 (footnote omitted) (quoting § 1061, 118 Stat. at 3684).

Congress responded quickly by passing legislation in August 2007 to significantly restructure the PCLOB.[280] Under the new statute, the PCLOB is an independent agency to be composed of five members, four of whom are part time from outside the government and the fifth, the chairperson, is the full time member.[281] All five members are appointed by the President and confirmed by the Senate for a term of six years to prevent wholesale capture by a given Administration.[282] Its authorizing statute mandates that no more than three members can be from one political party with the other two chosen by the White House under consultation with Senate and House minority leadership.[283]

Despite these congressional efforts to force internal interagency oversight on intelligence issues, from 2007 until 2012, no members were ever appointed to the PCLOB.[284] In mid-2013, after significant pressure from both within and outside the Administration, the full board was nominated and confirmed.[285] Time will ultimately tell how effective the PCLOB will be as a source of productive tension within the national security arena. Working against it is the fact that "[f]our of the board members technically must be part time under the law; only [David] Medine, the fifth, can work on a full-time basis as chairman. The oversight body also lacks much of a workforce: At the moment it's mostly staff members on loan from other agencies."[286] Assuming PCLOB is capable of taking on such a huge responsibility,

---

280. *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801, 121 Stat. 266, 352 (2007) (codified as amended at 42 U.S.C. § 2000ee (Supp. I 2009)).

281. 42 U.S.C. § 2000ee(h)(1).

282. *Id.* § 2000ee(h)(2).

283. *Id.*

284. *See* Scott Shane, *The Troubled Life of the Privacy and Civil Liberties Oversight Board*, N.Y. TIMES BLOG (Aug. 9, 2012, 9:49 AM), http://thecaucus.blogs.nytimes.com/2012/08/09/the-troubled-life-of-the-privacy-and-civil-liberties-oversight-board; *see also* Michael Daniel, Danny Weitzner & Quentin Palfrey, *Senate Confirms Four Nominees to Privacy & Civil Liberties Board*, WHITEHOUSE.GOV BLOG (Aug. 3, 2012, 4:55 PM), http://www.whitehouse.gov//blog/2012/08/03/senate-confirms-four-nominees-privacy-civil-liberties-board.

285. *See* Jedidiah Bracy, *Medine's Confirmation Moves PCLOB Forward; Questions Remain About Cybersecurity Authority*, INT'L ASS'N PRIVACY PROFS. (June 1, 2013), https://www.privacyassociation.org/publications/2013_05_08_medines_confirmation_moves_pclob_forward_questions_remain_about.

286. Tony Romm, *Growing Pains for Privacy Watchdog PCLOB*, POLITICO (July 17, 2013, 11:58 PM), http://www.politico.com/story/2013/07/growing-pains-privacy-pclob-94388.html.

its success will be contingent on its members being included in national security related decision making and its ability to effectively wield power and influence on these issues.

2. *Oversight by High-Ranking Officials*

A second mechanism by which to construct checks and balances on the FBI is to have direct oversight over the Attorney General Guidelines by high-ranking members within the executive branch in order to create a separate source of responsibility and accountability for overreach. One such oversight effort has been the creation of an Office of the Inspector General (OIG) within agencies, including the DOJ.[287] Though the OIG has been a valuable check on agency activity, it is, as it currently stands, ill-equipped to be an effective check on the Attorney General Guidelines.

The OIG within the DOJ is a statutorily created position.[288] The Inspector General is appointed by the President, subject to Senate confirmation, and reports both to the Attorney General and Congress.[289] This structure was created in order to ensure maximum independence of the OIG within the agency. The mission of the Justice Department's OIG "is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel."[290] Under this language, investigating potentially illegal activities conducted pursuant to the Attorney General's Guidelines fits squarely within the OIG's mandate.

Despite the broad language, Dan Meyer, former Director for Whistleblowing and Transparency at the DOD, described the mandate as being much narrower in practice.[291] Meyer explained that, due to the resource constraints facing most OIGs, there is a limited amount of oversight that the office can provide.[292] Thus, OIGs often focus on activities that are both clearly illegal and easy to fix. For example, within the DOD, the OIG directs a substantial amount of its effort toward investigating corrupt defense contractors

287. Thanks to Dru Brenner-Beck for this insight and for countless others.

288. *About the Office*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, http://www.justice.gov/oig/about/ (last visited Mar. 14, 2014).

289. *Id.*

290. *Id.*

291. Telephone Interview with Dan Meyer, former Dir., Whistleblowing & Transparency, U.S. Dep't of Def. (May 24, 2013).

292. *Id.*

and other traditional forms of waste, fraud, and abuse.[293] Meyer described the OIG's authority as covering a sphere of activity, the center of which is comprised of clear-cut and easily identifiable instances of waste, fraud, and abuse, and the outer edges of which contain those questionably legal activities that require significant resources to investigate fully.[294] Because of the resource constraints that the OIG invariably faces, the office is motivated to focus on the center of the sphere instead of the outer edges.

If Meyer's theory is correct, broad shifts in mission and process that raise difficult questions regarding the scope of legally authorized behavior often evade Inspector General review. This view is supported by Professors Posner and Vermeule, who note that

> "the Inspectors General have been more or less effective at what they do, but what they do has not been effective. That is, they do a relatively good job of compliance monitoring, but compliance monitoring alone has not been that effective at increasing governmental accountability. Audits and investigations focus too much on small problems at the expense of larger systemic issues."[295]

Fixing the oversight problem is eminently possible. Currently, Inspector General's offices are understaffed and operate with an extremely broad mission that includes going after people who are cheating the United States Government and also going after the United States Government for potentially cheating Americans of their civil liberties. These are jobs that are fundamentally different in both the scope and the resources needed.

Creating an OIG for internal affairs and an OIG for external affairs is one solution to this problem. An OIG for internal affairs ensures that the contractors and the employees are clean and that there is no waste, fraud, and abuse among programs and employees. An OIG for external affairs would be specifically responsible for monitoring programs that encroach on the rights of the public. An OIG for external affairs within the Justice Department would be responsible for monitoring the evolution and implementation of the Attorney General Guidelines and other such national security efforts. In this function, the OIG for external affairs becomes the designated

---

293. *About Us*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., http://www.dodig.mil/About_Us/index.html (last visited Mar. 14, 2014).

294. Telephone Interview with Dan Meyer, *supra* note 291.

295. POSNER & VERMEULE, *supra* note 254, at 87 (quoting William S. Fields, *The Enigma of Bureaucratic Accountability*, 43 CATH. U. L. REV. 505, 516-17 (1994) (reviewing PAUL C. LIGHT, MONITORING GOVERNMENT: INSPECTORS GENERAL AND THE SEARCH FOR ACCOUNTABILITY (1993))).

public advocate within an agency. Importantly, in this role, the OIG for external affairs functions very similarly to the PCLOB. However, redundancy, especially when it comes to protecting civil liberties, can be virtue.

3. *Dissent Channel: Whistleblowing*

A third mechanism by which to create internal checks and balances is, as Professor Neal Katyal calls them, "dissent channel[s]."[296] Katyal illustrates the value of dissent in practice through the example of the State Department's "Dissent Channel," which offers "any officer in any embassy the ability and power to disagree with the position taken by the ambassador or high-ranking officials."[297] Unlike the State Department, the DOJ does not have an established dissent channel, and the addition of one could prove useful.

The State Department's Dissent Channel allows individuals within the agency to share their dissenting views anonymously with the agency's well-regarded Policy Planning Staff.[298] The Policy Planning Staff is then responsible for funneling the most important concerns to higher-level people within the agency, including the Secretary of State.[299] This Dissent Channel is, by Katyal's account, a successful method of ensuring the agency operates interactively instead of entirely through command-and-control leadership. Moreover, it creates an opportunity for private dissent in an environment where, because of the confidentiality that attaches to official business, public dissent is not possible.

The DOJ does not have an established dissent channel and, as one government official explained off the record, dissent is not encouraged within the FBI.[300] This is because, like the State Department, the institutional mandate does not support it, requiring instead strict command-and-control leadership. Also like the State Department, the secrecy that the FBI sometimes needs to operate under prohibits more public forms of dissent. These similarities make a State Department-styled Dissent Channel within the Justice Department a potentially valuable intra-agency check and balance.

---

296. Katyal, *supra* note 262, at 2339.
297. *Id.* at 2328.
298. *Id.*
299. *Id.* at 2328-29.
300. Telephone Interview with anonymous source (May 28, 2013).

Another mechanism to support internal dissent is to promote whistleblower protections. The Civil Service Reform Act of 1978 (CSRA) first established statutory whistleblower protections for federal employees to encourage disclosure of government illegality, waste, fraud, and abuse.[301] Soon after, the reforms were narrowed through a sequence of court decisions. This prompted congressional revisions of the law in 1989, 1994, and, most recently, in 2012 with the Whistleblower Protection Enhancement Act (WPEA).[302]

Despite this set of reforms, whistleblower protections for the intelligence community remain weak. Section 105 of the WPEA exempts "the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office," and any other agency "as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities, provided that the determination be made prior to a personnel action."[303] After the Snowden leaks became public, some members of the press and public-interest organizations pointed to this weakness as one reason for the public nature of the leak.[304]

Furthermore, even national security whistleblowers who do not fear reprisal by their employers are unable to alert the public to potentially illegal activities because such activities are oftentimes classified and cannot be disclosed without violating federal law.[305] And though a whistleblower cannot legally be punished for

---

301. *See* Civil Service Reform Act of 1978, Pub. L. No. 95-454, § 101(a), 92 Stat. 1111, 1116 (1978) (codified as amended at 5 U.S.C. § 2302 (2006)).

302. *See* Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112-199, 126 Stat. 1465 (2012) (codified as amended at 5 U.S.C. § 2302 (2012)).

303. Whistleblower Protection Enhancement Act § 105.

304. *See, e.g.*, Pema Levy, *Loopholes Exclude Intelligence Contractors like Snowden from Whistleblower Protections*, INT'L BUS. TIMES (June 11, 2013), http://www.ibtimes.com/loopholes-exclude-intelligence-contractors-snowden-whistleblower-protections-1301913; HUMAN RIGHTS WATCH, HUMAN RIGHTS WATCH STATEMENT ON U.S. PROTECTION OF WHISTLEBLOWERS IN THE SECURITY SECTOR 2, 10 (2013), *available at* http://www.hrw.org/sites/default/files/related_material/HRW_Statement_on_US_Protection_of_Whistleblowers_in_the_Security_Sector_6-18-13_0.pdf.

305. *See* Espionage Act of 1917, 18 U.S.C. §§ 793-99 (2000); *see also* Jamie Sasser, Comment, *Silenced Citizens: The Post*-Garcetti *Landscape for Public Sector Employees Working in National Security*, 41 U. RICH. L. REV. 759, 760-61 (2007).

disclosing clearly illegal practices that are otherwise classified,[306] this loophole requires a whistleblower to conduct the impossible task of determining that a given activity is clearly illegal *without* being able to take the issue to court for such a determination. A whistleblower that discloses the existence of classified information documenting practices or activities that are *most likely illegal* is faced with potential criminal repercussions unless she discloses such information to a clearance-holding member of the United States Government.

The difficulty posed by classified information and the fear of reprisal makes dissent in the national security arena a complex and dangerous affair and, therefore, an unlikely occurrence. Failure to facilitate dissent within the FBI represents a failed opportunity for forcing intra-agency deliberation and allows for unchecked agency norm entrepreneurship.

Intra-agency checks and balances, such as the creation of dissent channels within the FBI and statutory amendments to the WPEA to extend whistleblower protections to the intelligence community, are, given the political climate in the wake of the Snowden NSA scandal, increasingly possible.[307] There is significant attention directed to the Administration's treatment of whistleblowers and growing recognition of the need for whistleblowers within the national security arena. This attention may create enough momentum to force Congress to revisit the WPEA and motivate an agency overhaul to promote both transparency and dissent within the FBI and the DOJ more broadly.

Of course, shadow administrative constitutionalism is hardly the result of failures within the executive branch alone. Next, I explore the judicial failures that led to shadow administrative constitutionalism.

---

306. *See* 3 C.F.R. § 1.7 (2004), *reprinted in* 50 U.S.C. § 435 (2006) (establishing that clearly illegal activity cannot be properly classified in the first instance).

307. This references both the NSA PRISM scandal and the NSA link to the blanket Verizon FISC order. *See* Amy Davidson, *America Through the N.S.A.'s Prism*, NEW YORKER BLOG (June 7, 2013, 2:00 AM), http://www.newyorker.com/online/blogs/closeread/2013/06/america-through-the-nsas-prism.html.

B. Interbranch Deliberation

1. *Judicial Intervention*

The Church Committee, reflecting on the *Keith* decision, emphasized the importance of judicial intervention in the national security arena when it reminded the public that warrantless wiretapping "had been permitted by successive presidents for more than a quarter of a century without 'guidance from the Congress or a definitive decision of the Courts.'"[308] Unfortunately, there are three barriers to judicial intervention that facilitate shadow administrative constitutionalism in the national security arena: the lack of judicially enforceable rights, the standing hurdle, and the growth of executive privilege.

a. Judicially Enforceable Rights

By the time the Civiletti Guidelines were issued in 1980, the DOJ made eminently clear that the Attorney General Guidelines were "solely for the purpose of internal Department of Justice guidance"[309] and would otherwise be legally binding. Specifically, the Guidelines made clear that "[t]hey are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any manner, civil or criminal."[310] Such rights-limiting language prevents any injured party from using the governing document of the FBI to enforce the self-imposed limitations on the Bureau's power.

---

308. S. REP. NO. 94-755, bk. I, at 11 (1976) (quoting United States v. U.S. District Court (*Keith*), 407 U.S. 297, 299 (1972)).

309. S. REP. NO. 97-682 app. D at 516 (1983); *see also supra* note 105, at 787.

310. S. REP. NO. 97-682 app. D at 516. As Elliff describes:

> Although the Levi guidelines contained no such language, the 1979 FBI charter bill expressly barred judicial enforcement of either the proposed statutory standards or the Attorney General's guidelines that the bill required for FBI investigations. These provisions in the guidelines and the charter bill parallel the Supreme Court's decision in *United States v. Caceres*, where the Court held that technical violations of Internal Revenue Service guidelines for undercover investigations should not lead to reversal of a conviction on either due process or statutory grounds.

Elliff, *supra* note 105, at 787 (footnotes omitted).

b. The Standing Hurdle

The lack of judicially enforceable rights is not, however, the only problem. Those who might bring a First Amendment claim based on the surveillance authorized by the Attorney General Guidelines face immense difficulty simply getting into court.[311] One of the primary problems with surveillance is that it has the power to coerce people into self-censorship—or chilled speech. This makes surveillance, fundamentally, a First Amendment issue and a prime subject for constitutional litigation. As our communications are increasingly subject to the prying eyes of the government, our ability to speak freely is directly curtailed. However, after the Supreme Court's decision in *Laird v. Tatum*, litigants suing under the First Amendment theory of chilled speech are subject to a high standing bar that, more often than not, prevents them from having their case heard at all.

The first mention of the term "chill" in Supreme Court jurisprudence occurred in 1952 in *Wieman v. Updegraff*, a case overturning an Oklahoma law that required all state employees to take a loyalty oath denying all affiliation, direct and indirect, with "any foreign political agency, party, organization or Government, or with any agency, party, organization, association, or group whatever which has been officially determined by the United States Attorney General or other authorized agency of the United States to be a communist front or subversive organization."[312] In an important concurrence, Justice Frankfurter argued that the loyalty oath had "an unmistakable tendency to chill that free play of the spirit which all teachers ought especially to cultivate and practice."[313] From that time to when the term "chilling effect" was first used in *Dombrowski v. Pfister*[314] thirteen years later, Professor Frederick Schauer argues that

311. And those who are able to get into court find themselves faced with judges who "frequently engage in a second-order inquiry about *how a policy came to be* instead of asking the first-order question *how a policy works on the ground*." Huq, *supra* note 202, at 889. Huq argues, "The extent of judicial reliance upon a logic of Separation of Powers as a crutch for the adjudication of counterterrorism cases is unparalleled." *Id.* This faith in the separation of powers, when combined with Eskridge and Ferejohn's urging of judicial deference in matters of administrative constitutionalism, creates layers of walls within the judicial branch, preventing litigation of the substantive issues at the heart of national security litigation.

312. 344 U.S. 183, 186 (1952).

313. *Id.* at 195 (Frankfurter, J., concurring).

314. 380 U.S. 479, 487 (1965).

the term evolved from an "emotive argument into a major substantive component of first amendment [sic] adjudication."[315]

However, after *Laird v. Tatum*, litigating on the basis of chilling effects has become difficult. *Tatum* requires litigants to first prove that the surveillance in question led to a cognizable harm before they will be granted standing and further held that "the mere existence . . . of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose" was simply not a cognizable harm.[316]

As a result of *Tatum*, before an individual can bring a First Amendment claim against FBI based on the authorizations of the Attorney General Guidelines, she must first prove that she has been harmed by the often-secret surveillance.[317] Because of the difficulty of first affirmatively identifying that one is the subject of government surveillance in order to allege a cognizable harm under the law, such litigation has been made increasingly unlikely under *Tatum*.

For example, in 2005, *The New York Times* exposed the President's Surveillance Program (PSP), a program developed after 9/11 that secretly authorized the NSA to intercept "the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to Al Qaeda."[318] "Additionally, the NSA told Congress that privileged communications, such as those between an attorney and her client, would not be 'categorically excluded' from interception."[319]

This discovery led prominent civil rights organizations, including the American Civil Liberties Union (ACLU), to file

---

315. Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 685 (1978) (footnote omitted); *see also* Baird v. State Bar of Ariz., 401 U.S. 1, 6-7 (1971); Keyishian v. Bd. of Regents, 385 U.S. 589, 603-04 (1967); Lamont v. Postmaster Gen. of the U.S., 381 U.S. 301, 307 (1965); Baggett v. Bullitt, 377 U.S. 360, 372 (1964).

316. Laird v. Tatum, 408 U.S. 1, 10 (1972).

317. *Id.* at 14.

318. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html.

319. Kali Borkoski, *Suing over Surveillance Secrets*, SCOTUSBLOG (Oct. 29, 2012, 9:33 AM), http://www.scotusblog.com/2012/10/suing-over-surveillance-secrets/.

lawsuits against the government arguing that their speech was chilled because their communications were likely targets of the surveillance program.[320] The ACLU filed on behalf of itself and a group of journalists, scholars, and other organizations that regularly communicate with likely targets of the PSP.[321] Importantly, none of the plaintiffs had evidence that they were in fact the subject of NSA surveillance.[322] This was a fact that only the government knew and would not disclose. The Supreme Court held that, without this information, the plaintiffs lacked standing to pursue their case.[323]

The standing barrier created by *Tatum* is especially problematic given the nature of surveillance today. Surveillance today no longer presents viable Fourth Amendment claims because so much of our most personal information is mediated through third parties, and the third-party doctrine limits the extent of Fourth Amendment protections.[324] While Justice Sotomayor's concurrence in *United States v. Jones* provides some indication that this doctrine may be up

---

320. *See* Complaint at 13, Ctr. for Constitutional Rights v. Bush, No. 06-cv-313 (S.D.N.Y. Jan. 17, 2006), *available at* http://ccrjustice.org/files/CCR_NSA_Complaint_01_06.pdf.

321. *ACLU v. NSA: The Challenge to Illegal Spying*, ACLU, http://www.aclu.org/national-security/aclu-v-nsa-challenge-illegal-spying (last visited Mar. 14, 2014).

322. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013).

323. *Id.* at 1152. In a recent development, the government has, for the first time, notified a criminal defendant, Jamshid Muhtorov, that evidence obtained from a warrantless wiretap is expected to be used against him. Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES (Oct. 26, 2013), http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?_r=0. The disclosure is expected to "set up a Supreme Court test of whether such eavesdropping is constitutional." *Id.*

324. The third-party doctrine was articulated by the Supreme Court in *United States v. Miller*, where it held:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

425 U.S. 435, 443 (1976). The third-party doctrine has suffered quite an assault at the hands of the legal academy. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-64 (2007); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976 (2007). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009).

for reconsideration by the Supreme Court,[325] until that time, the Fourth Amendment no longer provides a powerful source of legal recourse against the growth of surveillance authority. As a result, now, more than ever, the chilling effects doctrine must be revived in order to provide a First Amendment backstop to the growing problem of government surveillance.

c. Executive Privilege

As Professor Heidi Kitrosser describes, "A claim of executive privilege is generally a claim by the President of a constitutional right to withhold information."[326] It is a claim whose authority lies not in the text of the Constitution or of any specific law, but rather in the "notion that some information requests effectively infringe on the President's Article II powers, threatening his ability to receive candid advice or to protect national security."[327]

Executive privilege as a means of obfuscation facilitates shadow administrative constitutionalism by preventing judicial oversight. Professor Jack Balkin first made this claim nearly ten years ago when he argued that, increasingly

> we exclude more and more executive action from judicial review on the twin grounds of secrecy and efficiency. . . . [A]n independent judiciary plays an important role in making sure that zealous officials do not overreach. If the executive seeks greater efficiency, this requires a corresponding duty of greater disclosure before the fact and reporting after the fact to determine whether its surveillance programs are targeting the right people or are being abused.[328]

The courts have not taken heed to his warning.

In the wake of the disclosure of the PSP, there was one case that survived the extremely high standing bar set in *Tatum*. In *Al-Haramain Islamic Foundation v. Bush*, an Islamic charity based in Oregon discovered that the government inadvertently sent them classified documents demonstrating that their communications were

325. 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

326. Heidi Kitrosser, *Secrecy and Separated Powers: Executive Privilege Revisited*, 92 IOWA L. REV. 489, 491-92 (2007).

327. *Id.* at 492.

328. Balkin, *supra* note 237, at 23.

subject to warrantless surveillance.[329] With proof that they were in fact subject to surveillance, Al-Haramain proceeded to court. However, the government argued that the state-secrets privilege prevented the introduction of the classified documents and permitted the government to avoid acknowledging the existence of the surveillance program.[330] Despite the fact that the classified information had already been disclosed (and in seemingly direct conflict with the government's otherwise settled third-party doctrine), the Ninth Circuit agreed with the government's position.[331]

The doctrinal barriers that prevent judicial intervention are significantly harder to overcome than the failures that stymie intrabranch checks and balances. This is in no small part due to the doctrine of stare decisis and the value of having binding precedent. Even judges who recognize the problems with the current system and wish to reassert their role in determining both small-"c" and ultimately large-"C" constitutional meaning cannot. Judge Colleen McMahon expressed her frustration with the state-secrets privilege in a court opinion, saying, "I can find no way around the thicket of laws and precedents that effectively allow the Executive Branch of our Government to proclaim as perfectly lawful certain actions that seem on their face incompatible with our Constitution and laws, while keeping the reasons for its conclusion a secret."[332] As a result, without a major shift in the doctrine, the judiciary will be limited in its ability to provide useful oversight.

2. *Congressional Oversight*

Congress is also capable of providing a powerful check on agency norm entrepreneurship. As the Church Committee reminded us, "[T]he Constitution provides for a system of checks and balances and interdependent power as between the Congress and the executive

329. Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1194-95 (9th Cir. 2007).

330. *Id.* at 1197.

331. *Id.* at 1203. The court agreed to allow the case to proceed if plaintiffs were able to prove standing without the introduction of the classified document that indicated Al-Haramain was subject to government surveillance. *Id.* at 1205. Plaintiffs were able to introduce non-classified evidence supporting their surveillance claims; however, the case was ultimately still thrown out in the Ninth Circuit because the government argued and the court conceded that the government had not waived sovereign immunity. *Id.* at 1202-03.

332. N.Y. Times Co. v. U.S. Dep't of Justice, 915 F. Supp. 2d 508, 515-16 (S.D.N.Y. 2013).

branch."[333] The Committee warned that a Congress that doesn't act, creating a "lack of clear legislation defining the authority for permissible intelligence activities," violates the Constitution because, "[a]bsent clear legal boundaries for intelligence activities, the Constitution has been violated in secret and the power of the executive branch has gone unchecked, unbalanced."[334]

Despite this warning, Congress failed to develop a legislative solution to FBI governance. Instead, it has left the Guidelines in place as "a signature pronouncement of the nation's top legal officer" representing "what the Attorney General thinks is the appropriate balance between the government's duty to prevent crime and to deter threats to the national security and the protection of the rights of Americans under the Constitution and the rule of law."[335] By deferring to the Attorney General to develop legal guidelines for its own investigative unit, Congress has abdicated a critical responsibility and facilitated the unregulated norm entrepreneurship embodied in the evolution of the Attorney General Guidelines.

Congressional abdication of its responsibility did not end there. Congress also failed to exercise its oversight authority. For example, the Judiciary Committees of both the House and the Senate have oversight authority of the FBI. Through regular and rigorous oversight hearings on the Attorney General Guidelines, Congress could have forced a dialogue about the norms embedded in and introduced through the Guidelines. Instead, there has been no mandatory or systematic oversight carried out with respect to the Attorney General Guidelines. Emblematic of the problem, in 2008, at a Senate hearing, Senator Bond, Vice Chairman of the Judiciary Committee, thanked the FBI for sharing an advance copy of the Guidelines, saying, "I'm pleased the Department of Justice and the FBI have taken the unprecedented step of consulting with Congress prior to the adoption of the guidelines."[336] That such communication

333. S. REP. NO. 94-755, bk. I, at 40 (1976).

334. *Id.* at 16.

335. *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. 2 (2008) [hereinafter *Guidelines for Investigations & Intelligence*] (statement of Sen. John D. Rockefeller IV, Chairman, S. Select Comm. on Intelligence).

336. *Id.* at 3 (statement of Sen. Christopher S. Bond, Vice Chairman, S. Select Comm. on Intelligence). Of course, the consultation wasn't made easy. According to Senator Rockefeller, "The Justice Department's decision to prohibit the Committee from retaining a copy of the draft guidelines in preparing for this hearing and to restrict their public distribution has been unhelpful and has

between Congress and DOJ is unprecedented speaks to the dearth of congressional oversight on the evolution of the Attorney General Guidelines to date.

The solution to a lack of congressional oversight is conceptually easy but practically difficult. It requires Congress to pass legislation governing the FBI and regularly exercise its statutory oversight authority, both of which require significant political capital and effort. However, the Snowden scandal may have created the momentum necessary to motivate congressional action in this area. Senator Ron Wyden recently echoed this sentiment while imploring his colleagues to act stating, "'If we do not seize this unique moment in out [sic] constitutional history to reform our surveillance laws and practices we are all going to live to regret it.'"[337]

C. Public Transparency

The Church Committee made clear that "[s]ecrecy has shielded intelligence activities from full accountability and effective supervision."[338] The intervening years since the Church Committee released its report have been marked again by an increase in secrecy and a decrease in public awareness of the FBI's intelligence-gathering activities. As noted earlier, the Attorney General Guidelines are not released for public inspection and review before they are formally issued.[339] In a 2008 hearing, Senator Rockefeller noted this on the record during a congressional hearing stating, "[T]he proposed guidelines have not been publicly released . . . for broader debate and broader comment."[340]

Given that these Guidelines are increasingly unclassified upon issuance, there is no reason why they should not be unclassified and available for public deliberation *before* they are issued. A notice-and-comment-style process should be required of the DOJ when it issues its Attorney General Guidelines and when the FBI issues its

---

unnecessarily complicated our review of them." *Id.* at 2 (statement of Sen. John D. Rockefeller IV, Chairman, S. Select Comm. on Intelligence).

337. Perry Stein, *Wyden: If We Do Not Reform Our Surveillance Laws, We Will Live to Regret It*, TPM LIVEWIRE (July 23, 2013, 11:35 AM), http://talkingpointsmemo.com/livewire/wyden-if-we-do-not-reform-our-surveillance-laws-we-will-live-to-regret-it (quoting Sen. Ron Wyden).

338. S. REP. NO. 94-755, bk. I, at 16.

339. *See supra* Section II.C.

340. *Guidelines for Investigations & Intelligence*, *supra* note 335, at 1.

DIOGs. Such a process would allow *ex ante* public discussion of the appropriate principles and procedures that govern the FBI.

The failure of public transparency, congressional oversight, judicial intervention, and internal executive branch checks and balances allowed for the insular agency decision making and the norm entrenchment that marked the evolution of the Attorney General Guidelines. But this is not inevitable. As this Part shows, we can force deliberation by manufacturing mechanisms to create public transparency, require congressional oversight, and institute intraexecutive checks and balances.

CONCLUSION

This Article begins to tackle an under-theorized area in legal scholarship: the role of administrative agencies, often in isolation, in articulating the contours of constitutional protections in the area of national security. Our national security law is determined largely by administrative agencies—be it the DOJ, the DOD, the CIA, the NSA, or the various fiefdoms within each of these agencies.

While the War on Terror has led to significant interest in the growth of Executive Power, this interest has largely focused on the roles of the President and his closest advisors in determining the contours of the President's constitutional authority. However, given the high profile nature of presidential power grabs, many of these interpretations of executive authority ultimately are reviewed by the Supreme Court or at least reviewed by the public. As we saw with the series of Supreme Court decisions on the legal rights of Guantanamo detainees[341] and the President's renewed promises, in the face of serious public pressure, to close Guantanamo and rein in

341. Hamdi v. Rumsfeld, 542 U.S. 507, 510, 533 (2004) (holding that a citizen detainee challenging detention under the Fifth Amendment due process clause has the right to "receive notice of the factual basis for his classification, and a fair opportunity to rebut the Government's factual assertions before a neutral decisionmaker"); Rasul v. Bush, 542 U.S. 466, 484 (2004) (holding that the federal habeas corpus statute granted federal courts jurisdiction to hear claims of noncitizen detainees held at Guantanamo); Hamdan v. Rumsfeld, 548 U.S. 557, 567 (2006) (finding the military commissions created under the Detainee Treatment Act to be illegal); Boumediene v. Bush, 553 U.S. 723, 732 (2008) (holding that Guantanamo detainees have constitutional rights to challenge their detention in United States courts).

drone warfare,[342] serious expansion of presidential power is often subject to checks and balances.

Comparatively, administrative agencies operate under the radar—not necessarily making the big decisions on detention authority or warrantless wiretapping programs, but making the smaller decisions on how much the FBI can do without obtaining a warrant. These seemingly smaller things remain outside of public purview and escape public deliberation.

Administrative constitutionalism presents a democratic process by which to arrive at constitutional meaning. However, agency norm entrepreneurship that is not followed by robust deliberation threatens to allow agencies, the least accountable members of our tripartite government, the power to create and entrench constitutional norms that ultimately inform the development of constitutional law. Building structural solutions to force deliberation can ensure the legitimacy of administrative constitutionalism.

342. Tom Curry, *Obama Reframes Counterterrorism Policy with New Rules on Drones*, NBC NEWS (May 23, 2013, 11:00 AM), http://nbcpolitics.nbcnews.com/_news/2013/05/23/18448515-obama-reframes-counterterrorism-policy-with-new-rules-on-drones?lite.