University of Michigan Law School
University of Michigan Law School Scholarship Repository

Articles | Faculty Scholarship

2015

Intelligence Legalism and the National Security Agency's Civil Liberties Gap

Margo Schlanger
University of Michigan Law School, mschlan@umich.edu

Available at: https://repository.law.umich.edu/articles/1410

Follow this and additional works at: https://repository.law.umich.edu/articles

 Part of the Constitutional Law Commons, National Security Law Commons, President/Executive Department Commons, and the Privacy Law Commons

Recommended Citation
Schlanger, Margo. "Intelligence Legalism and the National Security Agency's Civil Liberties Gap." Harv. Nat'l Sec. J. 6 (2015): 112-205.

This Article is brought to you for free and open access by the Faculty Scholarship at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Articles by an authorized administrator of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

ARTICLE

Intelligence Legalism and the National Security Agency's Civil Liberties Gap

Margo Schlanger[*]

[*] Henry M. Butzel Professor of Law, University of Michigan. I have greatly benefited from conversations with John DeLong, Mort Halperin, Alex Joel, David Kris, Marty Lederman, Nancy Libin, Rick Perlstein, Becky Richards, and several officials who prefer not to be named, all of whom generously spent time with me, discussing the issues in this article, and many of whom also helped again after reading the piece in draft. I would also like to extend thanks to Sam Bagenstos, Rick Lempert, Daphna Renan, Alex Rossmiller, Adrian Vermeule, Steve Vladeck, Marcy Wheeler, Shirin Sinnar and other participants in the 7th Annual National Security Law Workshop, participants at the University of Iowa law faculty workshop, and my colleagues at the University of Michigan Legal Theory Workshop and governance group lunch, who offered me extremely helpful feedback. Jennifer Gitter and Lauren Dayton provided able research assistance. All errors are, of course, my responsibility.

Copyright © 2015 by the Presidents and Fellows of Harvard College and Margo Schlanger.

Abstract

Since June 2013, we have seen unprecedented security breaches and disclosures relating to American electronic surveillance. The nearly daily drip, and occasional gush, of once-secret policy and operational information makes it possible to analyze and understand National Security Agency activities, including the organizations and processes inside and outside the NSA that are supposed to safeguard American's civil liberties as the agency goes about its intelligence gathering business. Some have suggested that what we have learned is that the NSA is running wild, lawlessly flouting legal constraints on its behavior. This assessment is unfair. In fact, the picture that emerges from both the Snowden and official disclosures is of an agency committed to legal compliance, although both minor and major noncompliance is nonetheless frequent. A large surveillance compliance apparatus is currently staffed by hundreds of people in both the executive and judicial branches. This infrastructure implements and enforces a complex system of rules, not flawlessly but with real attention and care. Where an authoritative lawgiver has announced rights or rights-protecting procedures, the compliance apparatus works—to real, though not perfect effect—to effectuate those rights and to follow those procedures.

Of course errors, small and large, occur. But even if perfect compliance could be achieved, it is too paltry a goal. A good oversight system needs its institutions not just to support and enforce compliance but also to design good rules. Yet the offices that make up the NSA's compliance system are nearly entirely compliance offices, not policy offices; they work to improve compliance with existing rules, but not to consider the pros and cons of more individually-protective rules and try to increase privacy or civil liberties where the cost of doing so is acceptable. The NSA and the administration in which it sits have thought of civil liberties and privacy only in compliance terms. That is, they have asked only "*Can* we (legally) do X?" and not "*Should* we do X?" This preference for the *can* question over the *should* question is part and parcel, I argue, of a phenomenon I label "intelligence legalism," whose three crucial and simultaneous features are imposition of substantive rules given the status of law rather than policy; some limited court enforcement of those rules; and empowerment of lawyers. Intelligence legalism has been a useful corrective to the lawlessness that characterized surveillance prior to intelligence reform, in the late 1970s. But I argue that it gives systematically insufficient weight to individual liberty, and that its relentless focus on rights, and compliance, and law has obscured the absence of what should be an additional focus on interests, or balancing, or policy. More is needed; additional attention should be directed both within the NSA and by its overseers to surveillance policy, weighing the security gains from surveillance against the privacy and civil liberties risks and costs. That

attention will not be a panacea, but it can play a useful role in filling the civil liberties gap intelligence legalism creates.

Part I first traces the roots of intelligence legalism to the last generation of intelligence disclosures and resulting reform, in the late 1970s. Part I then goes on to detail the ways in which intelligence legalism is embedded in both the Foreign Intelligence Surveillance Act of 1978 (FISA) and Executive Order 12,333, which govern American intelligence practices, and why the result is a civil liberties gap. Part II discusses the ways in which NSA's compliance and oversight institutions likewise embody intelligence legalism. I then move in Part III to some shortcomings of this system, and in particular the ways in which the law and NSA's compliance regulations and infrastructure fall short of full civil liberties policy evaluation. In Part IV, I examine some of the many reforms that have recently been proposed, analyzing those that might fill that gap. In light of the existing institutional arrangements, I sketch some thoughts on how they could do so most effectively.

Table of Contents

Introduction……116

I. Intelligence Legalism……120

A. *Origins* ……120
B. *FISA* ……123
C. *Executive Order 12,333* ……129

II. The NSA's Existing Compliance and Oversight Ecosystem……133

A. *NSA Offices* ……137
1. NSA Compliance Office ……137
2. NSA Office of Civil Liberties and Privacy ……140
3. NSA Office of Inspector General ……142
4. NSA Office of General Counsel ……144
B. *Department of Justice National Security Division (NSD)*……152
C. *Other Intelligence Oversight Offices*……158
D. *FISA Court* ……162
E. *PCLOB* ……166

III. The Liberty Gap ……172

A. *The Limited, Though Important, Reach of Legality* ……173
1. The Constitution ……173
2. Statutory Law……177
3. Executive Order……180
B. *Lawyers Are Not Civil Libertarians* ……183
C. *The Costs of Intelligence Legalism*……184
1. Intelligence Legalism Crowds Out Interest Balancing ……185
2. Intelligence Legalism and Legitimation ……186

IV. Reforms ……188

A. *NSA Office of Civil Liberties and Privacy* ……193
1. Maintaining Influence ……193
2. Maintaining Commitment ……196
B. *Civil Liberties/Privacy Official(s) in the White House* …… 199
C. *A Public Advocate in the FISA Court* ……201

Conclusion ……204

Introduction

The story has now been told many times: On March 10, 2004, President Bush's White House Counsel, Alberto Gonzales, and chief of staff, Andrew Card, went to the intensive care unit of the George Washington University Hospital to try to persuade the ill Attorney General, John Ashcroft, to sign off on continuing massive collection of Americans' internet metadata, a program started in October 2001. Deputy Attorney General James Comey had refused to reauthorize the program; its most recent authorization was scheduled to expire the next day. However, Comey got to his boss first, and Ashcroft refused to sign. Pushed hard by Gonzales and Card, and also by Vice President Cheney and his counsel, David Addington, Comey and several of his Department of Justice colleagues stood their ground and declined to ratify this domestic metadata collection based on the President's bare say-so.[1] This 2004 incident, the subject of much admiring later press for the DOJ lawyers,[2] is part of what won Comey, a Republican, his current appointment by President Obama to head the FBI.[3] This was a group of lawyers who stood up to extreme pressure to tell their client—the President—"no," loudly (if in secret) and backed by threat of group resignation. In a speech several years later to Intelligence Community lawyers, Comey talked about the need for his listeners to "stand[] in front of the freight train" when pushed by their clients to sign off on a collection technique or target they believe to be unlawful.[4] The hospital bed incident, live in audience members' minds, gave Comey credibility.

But what did this incident actually accomplish? Recent disclosures underscore that the dramatics were entirely out of scale to the actual, limited result, which was a pause—not a stop—to the challenged collection.[5] What

---

[1] For descriptions of the events, see, e.g., David Johnston & Scott Shane, *Notes Detail Pressure on Ashcroft Over Spying*, N.Y. TIMES, Aug. 17, 2007, at A14; Barton Gellman, *Conflict Over Spying Led White House to Brink*, WASH. POST, Sept. 14, 2008, at A1; JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 278-286 [hereinafter BAMFORD, THE SHADOW FACTORY]; OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY, ST-09-0002 WORKING DRAFT 42 (2009) [hereinafter 2009 NSA Draft IG Report], http://perma.cc/4E3N-HV7C.

[2] *See, e.g.*, Daniel Klaidman, *Palace Revolt*, NEWSWEEK (Feb. 5, 2006), http://perma.cc/X8TW-NANB (labeling the episode part of a "profile in courage"); Dan Eggen & Paul Kane, *Gonzales Hospital Episode Detailed*, WASH. POST (May 16, 2007), http://perma.cc/53D5-YYZ9.

[3] *See* Associated Press, *New Director James Comey Wants FBI 'Independent of All Political Forces,'* THE GUARDIAN (Oct. 28, 2013, 4:47 PM), http://perma.cc/53G6-HH3B (emphasizing that the 2004 event "symbolized a key piece of Comey's past").

[4] James B. Comey, *Intelligence Under Law*, 10 GREEN BAG 2D 439, 442 (2005).

[5] The most recent disclosures, made in response to an EFF FOIA request, were bundled together and posted at the ODNI's Tumblr (!), as Office of the Director of National Intelligence Public Affairs Office, *Newly Declassified Documents Regarding the Now-Discontinued NSA Bulk Electronic Communications Metadata Pursuant to Section 402 of the Foreign Intelligence Surveillance Act* (Aug. 11, 2014), http://perma.cc/3LJ5-6GD3. They evidence the government's position that the FISA Court was obligated to approve the internet metadata program without examination of its justification. *Memorandum of Law*

had previously been an entirely executive initiative was pushed into the FISA Court's tent by a massive expansion of FISA's pen register provision. The authority under which the collection proceeded, four months later, was new, but the program was the same.[6] Comey and his colleagues' actions were less standing down a freight train, and more the ordinary lawyers' task of assisting a client to make adjustments in order to accomplish operational goals using different methods. This was a compliance improvement—and it served rule-of-law values. But as far as the civil liberties impact, the change was all but symbolic.[7]

The mindset of Justice Department participants in the 2004 hospital bed incident—a stance I call "intelligence legalism"—is the topic of this Article. In her classic book, *Legalism: Law, Morals, and Political Trials*, Judith Shklar defined legalism as "the ethical attitude that holds moral conduct to be a matter of rule following, and moral relationships to consist of duties and rights determined by rules."[8] Legalism, Shklar observed, is the central shared commitment of members of the legal profession.[9] It is what underlies Tocqueville's much older observations about lawyers:

> If they prize freedom much, they generally value legality still more. They are less afraid of tyranny than of arbitrary power, and provided the legislature undertakes of itself to deprive men of their independence, they are not dissatisfied.[10]

Intelligence legalism brings lawyers' rule-of-law commitment into the realm of national security and surveillance, where secrecy molds its impact in a number of important ways. I see intelligence legalism's three crucial and simultaneous features as: imposition of substantive rules given the status of law rather than policy, limited court enforcement of those rules, and empowerment of lawyers. All three were in evidence in the 2004 drama. Yet it is no coincidence that that incident did not catalyze a civil liberties advance. In fact, this Article's core argument is that intelligence legalism,

---

and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes 3, Docket PR/TT [redacted] (FISA Ct. 2004), http://www.clearinghouse.net/chDocs/public/NS-DC-0028-0003.pdf [http://perma.cc/D5D4-2V9Y] ("First, once the Government certifies, as it has here, that the "information likely to be obtained" is relevant to the investigation, the Court's inquiry is properly at an end and the Application should be approved. Congress made the Government's certification on this point dispositive.").

[6] 2009 NSA Draft IG Report, *supra* note 1.

[7] For an even more skeptical view of the incident, see Marcy Wheeler, *George W. Bush's False Heroes: The Real Story of a Secret Washington Sham*, SALON (Aug. 14, 2014), http://perma.cc/B8UP-ZAHF.

[8] JUDITH SHKLAR, LEGALISM: LAW, MORALS, AND POLITICAL TRIALS 1 (1964)

[9] *Id.* at 1–2, 8 ("Legalism is, above all, the operative outlook of the legal profession, both bench and bar.").

[10] ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 250 (Barnes & Noble Publishing 2003) (1835), quoted in SHKLAR, LEGALISM, *supra* note 8, at 15.

though useful, gives systematically insufficient weight to individual liberty. Legalism legitimates liberty-infringing programs. And its relentless focus on rights and compliance and law (with a definition of law that includes regulation, executive orders, court orders, etc.) has obscured the absence of what should be an additional focus on interests, or balancing, or policy. That additional focus is necessary, I argue, for optimal policy, which I take to be the safeguarding of liberty where there is no cost, or acceptable cost, to security.

The 2004 hospital-bed confrontation arose out of what has grown to be a large surveillance compliance apparatus, currently staffed by hundreds of people in both the executive and judicial branches. This infrastructure implements and enforces a complex system of rules, not flawlessly but—at least in recent years—with real attention and care.[11] Where an authoritative lawgiver has announced rights or rights-protecting procedures, the compliance apparatus works, to real, though not perfect effect, to effectuate those rights and to follow those procedures. Of course errors, small and large, occur. Even if perfect compliance could be achieved, however, it is too paltry a goal. A good oversight system needs its institutions not just to support and enforce compliance but to design good rules. But as will become evident, the offices that make up the compliance system of the National Security Agency (NSA) are nearly entirely compliance offices, not policy offices; they work to improve compliance with existing rules, but not to consider the pros and cons of more individually-protective rules and try to increase privacy or civil liberties where the cost of doing so is acceptable. The NSA and the Intelligence Community (IC) more generally have thought of civil liberties and privacy only in compliance terms. That is, they have asked only "*Can* we (legally) do X?" and not "*Should* we do X?" This preference for *can* over *should* is part and parcel, I argue, of intelligence legalism. More is needed. Additional attention should be directed both within the NSA and by its overseers to the basic policy issues, weighing the security gains from surveillance against the privacy and civil liberties risks and costs. That attention will not be a panacea, but it can play a useful role in filling the civil liberties gap intelligence legalism creates.

This Article rests on the unprecedented security breaches and disclosures of the past months. These began on June 5, 2013, when the British newspaper *The Guardian* ran the first story revealing information from top secret documents leaked by former NSA contractor Edward Snowden.[12] In the months since, a squadron of news outlets—the *Guardian*, the *Washington Post*, the *New York Times*, *Der Spiegel*, *Le Monde*, *CBC*—have between them published dozens of revelations about the NSA's

[11] Here I agree with Michael A. Cohen, *Keith Alexander Needs a Hug*, FOREIGN POLICY (June 5, 2014), https://perma.cc/3SU9-7KJT. As he says, "One of the many ironies of the Snowden story is that the modern legal infrastructure that regulates the actions of the NSA is a significant liberal accomplishment."

[12] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 6, 2013), http://perma.cc/7943-FPCS.

activities.[13] And the federal government has offered unprecedented responsive disclosures,[14] in part to put out its side of the story, and in part because the leaks have eliminated the operational effectiveness of a good many secrets. Government officials too have become newly willing to discuss the operations of their offices.[15] With the nearly daily drip, and occasional gush, of once-secret policy and operational information, it is now possible to analyze and understand NSA activities, including the organizations and processes inside and outside the NSA that are supposed to safeguard American's civil liberties as the agency goes about its spying business. The paper leans heavily on the new disclosures, both official and unofficial.

Part I first traces the roots of intelligence legalism to the last generation of intelligence disclosures and resulting reform, in the late 1970s. Then, it details the ways in which intelligence legalism is embedded in both the Foreign Intelligence Surveillance Act of 1978 (FISA) and Executive Order 12,333, which governs American intelligence practices, and why the result is a civil liberties gap. Part II discusses the ways in which NSA's compliance and oversight institutions likewise embody intelligence legalism. I then move in Part III to explain why intelligence legalism predictably underweights civil liberties.

The Snowden disclosures and subsequent governmental policy discussions have evidently led to a renewed interest in the "should" question, in Congress and in the White House. The President himself responded to a question about surveillance at a press conference: "just because we can do something doesn't mean we necessarily should."[16] What will result is still

---

[13] For a chronology of both the disclosures and the underlying events, see *Timeline of NSA Domestic Spying*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/nsa-spying/timeline (last visited Nov. 7, 2014).

[14] *See* Office of the Dir. of Nat'l Intelligence, IC ON THE RECORD, http://perma.cc/VV8C-APSS (last visited Nov. 7, 2014).

[15] This Article has benefitted greatly from this willingness, because I was able to conduct interviews of numerous current and former government officials. These include telephone interviews of: John DeLong, Dir. of Compliance, Nat'l Sec. Agency (Oct. 8, 2013) [hereinafter DeLong Interview]; a senior IC attorney (Feb. 26, 2014) [hereinafter IC Attorney Interview]; Morton H. Halperin, former Special Assistant to the President (Oct. 14, 2014) [hereinafter Halperin Interview]; Alex Joel, Civil Liberties Protection Officer, Civil Liberties and Privacy Office, Office of the Dir. of Nat'l Intelligence (Jan. 31, 2014) [hereinafter Joel Interview]; Marty Lederman, former Deputy Assistant Attorney General, Office of Legal Counsel, U.S. Dep't of Justice (Oct. 10, 2014) [hereinafter Lederman Interview]; Nancy Libin, former Privacy and Civil Liberties Officer, U.S. Dep't of Justice (Oct. 18, 2013) [hereinafter Libin Interview]; Becky Richards, Civil Liberties and Privacy Officer, Nat'l Sec. Agency (July 14, 2014) [hereinafter Richards Interview]; and two White House officials (Aug. 18 & 22, 2014) [hereinafter White House Official Interviews].

[16] Full Transcript: President Obama's December 20 News Conference (Dec. 20, 2013), http://perma.cc/D5KF-GG8Q. *See also*, *e.g.*, Lisa Monaco, *Obama Administration: Surveillance Policies under Review* (Oct. 24, 2013), http://perma.cc/Q7SK-A3UJ ("We

unclear. But Presidential Policy Directive 28, the most definite policy document thus far, signals the possibility of some new, more liberty-protective, surveillance rules. PPD-28 also promises several reforms that take quite a different approach. Rather than announcing new rules, the relevant provisions specify an internal organizational strategy; they designate actors and processes to facilitate fuller internal consideration of the "should" question, down the line. Other extant reform proposals similarly focus on organizational assignments and processes rather than compliance-ready rules. In light of the existing institutional arrangements, Part IV sketches some thoughts on how this swathe of suggested reforms could be most effective.

I. Intelligence Legalism

A. Origins

The June 2013 *Guardian* piece, which explained the NSA's program of wholesale collection of information about domestic phone calls (though not the contents of the phone conversations themselves) had an analogue in Seymour Hersh's front-page 1974 *New York Times* exposure of massive domestic surveillance by the CIA, in violation of rules limiting the agency to foreign spying.[17] As in recent months, Hersh's first leak-supported exposé was followed by additional reporting and many official disclosures.[18] The lead role in the following "year of intelligence,"[19] 1975, was played by a special Senate Committee chaired by Senator Frank Church,[20] whose seven

---

want to ensure we are collecting information because we *need* it and not just because we *can*.").

[17] Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES (Dec. 22, 1974), *available at* https://perma.cc/FC7V-4WWW

[18] For official reports and disclosures, see, especially, ROCKEFELLER COMMISSION, COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES (1975), http://perma.cc/3UQH-GCUZ and many volumes of Church Committee Reports and testimony, all available at *Church Committee Reports*, ASSASSINATION ARCHIVES AND RESEARCH CTR., http://perma.cc/3T82-TC9R (last visited Oct. 18, 2014). The House counterpart to the Church Committee, the Pike Committee, never issued its report, but the full document was leaked to the Village Voice and also eventually published in Great Britain. *See* Aaron Latham, *The CIA Report the President Doesn't Want You to Read*, VILLAGE VOICE (Feb. 16, 1976), at 69; *How Kissinger, the White House, and the CIA Obstructed the Investigation*, VILLAGE VOICE (Feb. 23, 1976), at 59; THE PIKE COMMITTEE, CIA: THE PIKE REPORT (1977). For additional leaked disclosures, see, *e.g.*, Seymour M. Hersh, *Underground for the C.I.A. in New York: An Ex-Agent Tells of Spying on Students*, N.Y. TIMES (Dec. 29, 1974), *available at* http://perma.cc/UVJ6-6PMG; Seymour M. Hersh, *Aides Say Robert Kennedy Told of C.I.A. Castro Plot*, N.Y. TIMES (Mar. 9, 1975), *available at* http://perma.cc/Q6Y4-RVGB.

[19] Editorial, *The Year of Intelligence*, N.Y. TIMES (Feb. 8, 1975).

[20] The Church Committee was known formally as the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *See* S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE

volumes of reports and recommendations underlay much of the subsequent reform—including the formation of the still-operative congressional intelligence oversight committees, the passage of FISA, and the drafting of executive orders governing the intelligence enterprise.[21]

Reform took two basic approaches: disclosure and legalism. By disclosure I do not mean the kind of leaks and declassifications we have seen since 2013. The Church Committee, for example, did not chiefly urge a system of direct public accountability. Rather, it recommended that agencies running secret operations or intelligence surveillance make a long list of disclosures both to Congressional oversight committees and within the executive branch to the President and his staff,[22] and, as will be seen, to the Attorney General.[23] The idea was to defeat "plausible denials"[24] and the prior understanding with respect to both the Congress and the President that "[i]t's better for gentlemen not to know what's going on."[25] This would ease the path of accountability to higher-up appointees, who might have better judgment than those more deeply involved in surveillance, and to elected officials if not to their constituencies.

Legalism was a second reform priority: reformers' answer to the starkly apparent disinterest of federal intelligence officials in legal constraints on their activities.[26] Again looking to the Church Committee, the

---

ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-755 (1976) [hereinafter CHURCH COMMITTEE REPORT], http:// www.aarclibrary.org/publib/church/reports/contents.htm.

[21] *See, e.g.*, Anne Karalekas, *History of the Central Intelligence Agency*, *in* THE CENTRAL INTELLIGENCE AGENCY: HISTORY AND DOCUMENTS 11–119 (William M. Leary, ed. 1984); LOCH JOHNSON, A SEASON OF INQUIRY: THE SENATE INTELLIGENCE INVESTIGATION (1985); RICK PERLSTEIN, THE INVISIBLE BRIDGE: THE FALL OF NIXON AND THE RISE OF REAGAN (2014); KATHRYN OLMSTED, CHALLENGING THE SECRET GOVERNMENT: THE POST-WATERGATE INVESTIGATIONS OF THE CIA AND FBI (1996); Frederick A.O. Schwarz, Jr., *The Church Committee and a New Era of Intelligence Oversight*, 22 INTELLIGENCE AND NAT'L SEC. 270 (2007); KATHERINE A. SCOTT, REINING IN THE STATE: CIVIL SOCIETY AND CONGRESS IN THE VIETNAM AND WATERGATE ERAS (2013).

[22] *See, e.g.*, I CHURCH COMMITTEE REPORT, *supra* note 20, at 431, 441, 442, 444, 448–49 (recommendation 15, 24, 28, 31, 37); II CHURCH COMMITTEE REPORT, *supra* note 20, at 293, 331 (recommendation 68).

[23] *See, e.g.*, II CHURCH COMMITTEE REPORT, *supra* note 20, at 303, 308, 309, 310, 314, 315, 333 (recommendations 7(e), 13, 15, 17, 31, 35, 36, 70–74).

[24] *See* S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, AN INTERIM REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-465, at 11–12, 277–78 (1975) [hereinafter INTERIM CHURCH COMMITTEE REPORT], http://perma.cc/6BWS-A5XF.

[25] LEROY ASHBY & ROD GRAMER, FIGHTING THE ODDS: THE LIFE OF SENATOR FRANK CHURCH 471 (1994) (quoting Senator Leverett Saltonstall, as reported by Church); *see also, e.g.*, SAMUEL WALKER, PRESIDENTS AND CIVIL LIBERTIES FROM WILSON TO OBAMA: A STORY OF POOR CUSTODIANS 190 (2012).

[26] I lean on the evidence cited on the treatment of this issue in PERLSTEIN, THE INVISIBLE BRIDGE, *supra* note 21, at 330–32, 416-19, 520–24, 534–38, 678–79, and Frederick A.O. Schwarz, Jr., *The Church Committee and a New Era of Intelligence Oversight*, 22

Committee in its report highlighted testimony of "the man who for ten years headed FBI's Intelligence Division" that "never once did I hear anybody, including myself, raise the question: 'Is this course of action which we have agreed upon lawful, is it legal, is it ethical or moral.' We never gave any thought to this line of reasoning, because we were just naturally pragmatic."[27] Less dramatic, but perhaps even more telling, was the almost uncomprehending testimony of NSA deputy director Benson Buffham, facing questioning by Senator Walter Mondale, about a controversial NSA program:

> Mondale: "Were you concerned about its legality?"
> Buffham: "Legality?"
> Mondale: "Whether it was legal."
> Buffham: "In what sense? Whether that would have been a legal thing to do?"
> Mondale: "Yes."
> Buffham: "That particular aspect didn't enter into the discussion."[28]

A 1976 book by four civil libertarians, including former NSC staffer Mort Halperin, summarized the evidence in its title: *The Lawless State: The Crimes of the U. S. Intelligence Agencies*.[29] Legalistic reforms were designed to cure this documented disease.

Those reforms had three crucial and simultaneous features: imposition of new substantive rules given the status of law rather than policy; some limited court enforcement of those rules; and empowerment of lawyers. The first two of these features have received abundant attention: intelligence law was really born in the 1970s,[30] and has since blossomed.[31] It now has a body of precedent sufficient to justify a treatise[32] and casebooks.[33]

INTELLIGENCE AND NATIONAL SECURITY 270 (2007); FREDERICK A. O. SCHWARZ, JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR (2013).

[27] II CHURCH COMMITTEE REPORT, *supra* note 20, at 14 (statement of William Sullivan, Nov. 1, 1975, pp. 92–93).

[28] 5 *The National Security Agency and Fourth Amendment Rights: Hearing before the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 45 (1976) [hereinafter *Church Committee Hearings*] (statement of Benson Buffham, Deputy Director, NSA).

[29] MORTON H. HALPERIN, JERRY J. BERMAN, ROBERT L. BOROSAGE, CHRISTINE M. MARWICK, THE LAWLESS STATE: THE CRIMES OF THE U. S. INTELLIGENCE AGENCIES (1976).

[30] *See, e.g.*, United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297 (1972) (the "Keith case").

[31] *See, e.g.*, Fred F. Manget, *Another System of Oversight: Intelligence and the Rise of Judicial Intervention*, 39 STUDIES IN INTELLIGENCE 43–50 (1996).

[32] DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS (2d ed. 2012); JAMES CARR & PATRICIA BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE (2d ed. 2012).

The augmentation of lawyers' influence has gotten somewhat less attention.[34] But a crucial aspect of intelligence legalism is that even more than shifting power to the courts, it has shifted power to agency counsel and the Department of Justice, instituting internal rules governing intelligence operations and then deputizing the lawyers to see that those rules are implemented. Government lawyers accordingly loom very large in the reform documents of the late 1970s and thereafter. Over and over again, with dozens of specifics, the Church Committee recommended amplifying the authority and influence of lawyers within the executive branch.[35] The Committee summarized at the start of its domestic intelligence recommendations:

> Who should be accountable within the Executive branch for ensuring that intelligence agencies comply with the law and for the investigation of alleged abuses by employees of those agencies? . . . The Committee recommends that these responsibilities fall initially upon the agency heads, their general counsels and inspectors general, but ultimately upon the Attorney General.[36]

The specific domestic recommendations proposed to obligate the Attorney General to review procedures, authorize operations, and conduct

---

[33] *E.g.*, STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW (5th ed. 2011); NORM ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT (4th ed. 2011); STEPHEN DYCUS, WILLIAM C. BANKS, & PETER RAVEN-HANSEN, COUNTERTERRORISM LAW (2d ed. 2012); THOMAS M. FRANCK ET AL., FOREIGN RELATIONS AND NATIONAL SECURITY LAW: CASES, MATERIALS, AND SIMULATIONS (4th ed. 2011); GREGORY E. MAGGS, TERRORISM AND THE LAW: CASES AND MATERIALS (2d ed. 2009); WAYNE MCCORMACK, LEGAL RESPONSES TO TERRORISM (2d ed. 2008).

[34] Two major exceptions are JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 (2012) [hereinafter GOLDSMITH, POWER AND CONSTRAINT], and JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION (2007) [hereinafter GOLDSMITH, THE TERROR PRESIDENCY]. A few accounts of the work of the affected lawyers are available. *See* Laura A. Dickinson, *Military Lawyers on the Battlefield: An Empirical Account of International Law Compliance*, 104 AM. J. INT'L L. 1 (2010); Dorian D. Greene, *Ethical Dilemmas Confronting Intelligence Agency Counsel*, 2 TULSA J. COMP. & INT'L L. 91, 108 (1994); Harold Hongju Koh & Aaron Zelinsky, *Practicing International Law in the Obama Administration*, 35 YALE J. INTL. L. ONLINE 4 (2009); Mary C. Lawton, *Review and Accountability in the United States Intelligence Community*, OPTIMUM: J. PUB. SEC. MGMT. 101, 103 (Autumn 1993); JIM MCGEE & BRIAN DUFFY, MAIN JUSTICE: THE MEN AND WOMEN WHO ENFORCE THE NATION'S CRIMINAL LAWS AND GUARD ITS LIBERTIES 310-12 (1996); Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 486 (2006); Afsheen John Radsan, *Sed Quis Custodiet Ipsos Custodes: The CIA's Office of General Counsel?* 2 J. NAT'L SECURITY L. & POL'Y 201 (2008).

[35] *See, e.g.*, II CHURCH COMMITTEE REPORT, *supra* note 20, at 308–09, 315–16, 332–37. The Attorney General had a role, but a lesser one, in prior years. *See, e.g.*, Appendix A., Zweibon v. Mitchell, 516 F.2d 594, 673–75 (D.C. Cir. en banc, 1975).

[36] II CHURCH COMMITTEE REPORT, *supra* note 20, at 294.

investigations. Even more notable, the Church Committee proposed a similar role for the Attorney General with respect to foreign intelligence, far afield from the Attorney General's natural bailiwick of law enforcement and the FBI (which is at least nominally part of the Department of Justice):

> The Attorney General should be required to report the President and to the intelligence oversight committee(s) of Congress any intelligence activities which, in his opinion, violate the Constitutional rights of American citizens or any other provision of law and the actions he has taken in response. Pursuant to the Committee's Domestic Recommendations, the Attorney General should be made responsible for ensuring that intelligence activities do not violate the Constitution or any other provision of law.

Additional specifics abounded. For example, the Committee recommended that the Attorney General should advise the National Security Council and should even chair a counterintelligence subcommittee.[37] And the Church Committee's appreciation for the potential role of lawyers did not stop with the Attorney General. The reports included multiple recommendations, as well, to enhance the stature of intelligence agency general counsels—making their positions Senate confirmed, and requiring that they be consulted, have access to more information, and have investigatory powers.[38]

I have already mentioned the first reform that came from the Church Committee report: Congress's new permanent intelligence committees, established in 1975 and 1976.[39] In addition, the Committee's approach underlay both FISA and Executive Order 12,333. I move now to those two documents, and how legalism infuses them.

B. FISA

As originally enacted, FISA made two key innovations, both highly legalizing. First, the Act subjected all domestic foreign intelligence surveillance, and some such surveillance abroad, to analogues of domestic warrant procedure. Surveillance of covered communications would have to be authorized by a judicial officer—under FISA, a federal district judge appointed by the Chief Justice to the FISA Court—after the government demonstrated probable cause for the surveillance.[40] Second, FISA

---

[37] I CHURCH COMMITTEE REPORT, *supra* note 20, at 429, 431 (recommendation 6, 15).

[38] I CHURCH COMMITTEE REPORT, *supra* note 20, at 459–61; II CHURCH COMMITTEE REPORT, *supra* note 20, at 294, 308, 332–35.

[39] S. Res. 400, 94th Cong. (1976); H.R. Res. 658, 95th Cong. (1977).

[40] The probable cause determination under FISA is not, as in ordinary search warrants or Title III surveillance, probable cause to believe that a crime has been committed, but something less—probable cause "that the target of the surveillance or search is a 'foreign power' or an 'agent of a foreign power,' and that there is a nexus to the facility or place to be surveilled or searched." *See* 1 KRIS & WILSON, *supra* note 32, § 11:5. But the definition

introduced the idea of "minimization procedures"—rules "designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information"[41] that "concern[s] unconsenting United States persons."[42] The statutory "heart of minimization under FISA"[43] is the requirement that surveillance and retention processes be "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[44]

The FISA warrant requirement was, of course, borrowed from American criminal procedure. But the requirement of minimization procedures is far less familiar—indeed, it deviates foundationally from non-intelligence Fourth Amendment doctrine. In American criminal procedure, once the government gains lawful access to personal information, that information can usually be used for any lawful purpose—including purposes that would have invalidated the original access. So the government is authorized to search airplane travelers without any individualized suspicion, in order to be sure they are not, say, carrying a bomb that might bring down a plane.[45] Now, suppose that during that search, the government finds contraband that poses no aviation threat (drugs, perhaps, or a suspiciously large amount of currency). The evidence may then be used in a subsequent criminal prosecution, even though the very same search would have been illegal if its original purpose had been criminal prosecution. Likewise, if a police officer frisks a pedestrian in order to ameliorate the immediate threat of a gun, and along the way "plainly" feels drugs, the drugs are admissible in a criminal proceeding.[46] The foreign intelligence approach is different.[47] As

---

of "foreign power" and "agent of a foreign power" generally require some kind of nefarious conduct to justify a search targeting a U.S. citizen or resident. *See* 50 U.S.C. §§ 1801(a), (b); 1 KRIS & WILSON, *supra* note 32, § 8:2.

[41] In re Sealed Case, 310 F.3d 717, 731 (FISA Ct. Rev. 2002).

[42] 50 U.S.C. § 1801(h)(1); *see also, e.g.*, 50 U.S.C. § 1821(4); 50 U.S.C. § 1861(g); 50 U.S.C. § 1881a(e). In all things, FISA is complicated. For acquisitions under § 704, minimization is required for dissemination but not for acquisition or retention.

[43] 1 KRIS & WILSON, *supra* note 32, § 9:1.

[44] 50 U.S.C. § 1801(h)(1). *Compare* § 1821(4)(A) *with* § 1861(g)(2)(A).

[45] *See, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 47 (2000) (noting that the holding, which invalidated a vehicle checkpoint program, "d[id] not affect the validity of . . . searches at places like airports"); Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[W]here the risk to public safety is substantial and real, blanket suspicionless [sic] searches calibrated to the risk may rank as 'reasonable'—for example, searches . . . at airports.").

[46] Minnesota v. Dickerson, 508 U.S. 366, 377 (1993).

[47] *See* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1124–27 (2009) (laying out the differences between "collection limits" and "use limits," and setting out a variety of environments in which the law implements the latter); BENJAMIN WITTES, LAW AND THE LONG WAR 224 (2008) (advocating for "relatively easy access" to intelligence information coupled with "stricter rules" for "the use of that material."). I should note that in his 2008 book (published prior to

in the administrative search context, the regulation of information acquisition or collection is often very loose, with no requirement of individualized suspicion of wrongdoing in many situations. But, unlike with respect to criminal prosecution uses of evidence obtained by administrative search, the minimization procedures constrain what can happen next.[48]

Prior to the Snowden leaks, only one of the FISA minimization procedures—for information collected under a FISA Title I warrant[49]—had been declassified. Over the past months, the government has disclosed the terms of several others: for targeted surveillance of foreigners abroad (under FISA § 702),[50] the now-defunct internet metadata program (under FISA's pen register/trap-and-trace provision),[51] the ongoing telephony metadata

---

the FISA Amendments Act and the declassification of the various FISA minimization orders), Wittes disagrees with my characterization of surveillance law. He sees that law, rather, as "obsessed . . . with defining the circumstances of data acquisition," and disinterested in data use. *Id.* at 240.

[48] *See* 50 U.S.C. § 1805(c)(2)(A); 50 U.S.C. § 1824(c)(2)(A); 50 U.S.C. § 1861(g) (providing for minimization procedures for FISA warrants involving electronic surveillance, physical searches, and business record searches); 50 U.S.C. § 1881a(e); 50 U.S.C. § 1881b(b)(1)(D); 50 U.S.C. § 1881c(b)(4) (minimization procedures for targeted searches abroad). The pull of this minimization approach is so strong that when the government's internet metadata program was brought under the umbrella of FISA's pen/trap provisions, minimization procedures were part of the package, even though this part of the Act make no reference to minimization. *See* 50 U.S.C. §§ 1841-1848; Memorandum Opinion, No. PR/TT [Redacted], at 86 (FISA Ct. approx. June/July 2010) [hereinafter Bates 2010 PR/TT Opinion], http://www.clearinghouse.net/detail.php?id=13111 [http://perma.cc/N85U-UR5Q]; Opinion and Order, No. PR/TT [Redacted], at 43–44 (FISA Ct. July 2004) [hereinafter Kollar-Kotelly 2004 PR/TT Opinion], http://www.clearinghouse.net/detail.php?id=13107 [http://perma.cc/8649-AM73].

[49] The current NSA minimization rules for FISA Title I were approved by Attorney General Janet Reno on July 1, 1997. *See* NAT'L SEC. AGENCY ET AL, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE SP0018 Annex A, App. 1 (Jan. 25, 2011) [hereinafter USSID 18], http://perma.cc/VD3M-JP7G (Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (NSA)). The date appears at the end of the Appendix, after Section 8. The prior version of USSID 18 is dated July 27, 1993, but was released much later—and it includes the same (1997) version of these Standard Procedures, although they are differently titled. *See* NAT'L SEC. AGENCY ET AL, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE 18 Annex A, App. 1 (July 27, 1993) [hereinafter 1993 USSID 18], http://perma.cc/6Q4A-J9UG. It may be that minimization procedures are sometimes varied for different particular warrants. *See* USSID 18, *supra*, Annex A, Procedures Implementing Title I of the Foreign Intelligence Surveillance Act, Section 3 ("In some cases, the court orders are tailored to address particular problems, and in those instances the NSA attorney will advise the appropriate NSA offices of the terms of the court's orders. In most cases, however, the court order will incorporate without any changes the standardized minimization procedures set forth in Appendix I.").

[50] The minimization rules for FISA Section 702 are set forth in In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, 2008 WL 9487946, No. Misc. 08-01, at 10 (FISA Ct. 2008), http://www.clearinghouse.net/chDocs/public/NS-DC-0037-0001.pdf [http://perma.cc/9SJR-8GDG]. The minimization rules under Section 703 and 704 have not been either leaked or released.

[51] Bates 2010 PR/TT Opinion, *supra* note 48; Kollar-Kotelly 2004 PR/TT Opinion, *supra* note 48, at 43–44.

program (under FISA's business records provision),[52] as well as some others.[53] All of these minimization procedures support the conclusion that FISA's minimization procedure requirement is legalizing in several analytically distinct ways.

First, the procedures are themselves highly legalistic; they read like statutes or regulations. Second, the minimization procedures frequently use the strategy of designating a particular high official to make specified decisions.[54] Implementation then forces subordinate personnel into using the

---

[52] In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things From [Redacted], 2008 WL 9475145, No. BR 08-01 (FISA Ct. Jan. 2008), http://www.clearinghouse.net/chDocs/public/NS-DC-0037-0001.pdf [http://perma.cc/R9EJ-XJRF]. As this Article goes to press, the most recent of these orders declassified and available is In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things From [Redacted], No. BR 14-125 (FISA Ct. Sept. 2014), http://www.clearinghouse.net/chDocs/public/NS-DC-0067-0001.pdf [http://perma.cc/E888-3W3C]. An additional December 2014 order has not yet been declassified, but such information as is available is described and posted at http://www.clearinghouse.net/detail.php?id=14258 [http://perma.cc/EZJ7-2QFS].

[53] In ongoing litigation before the FISA Court, the United States recently declassified four different minimization procedures used by the FBI for physical and electronic searches since 1995 and 1997, respectively, as well as 2006 amendments to them. *See* Standard Physical Search Minimization Procedures, Exhibit A. In the Matter of the Application of the United States for an Order Authorizing Physical Search of a United States Person Agent of a Foreign Power, No. [omitted] (FISA Ct. 1995), http://www.clearinghouse.net/chDocs/public/NS-DC0008-0044.pdf [http://perma.cc/JK8D-FGPY]; Standard Physical Search Minimization Procedures, Exhibit A. In the Matter of the Application of the United States for an Order Authorizing Physical Search of a Non-United States Person Agent of a Foreign Power, No. [omitted] (FISA Ct. 1995), http://www.clearinghouse.net/chDocs/public/NS-DC-0008-0049.pdf [http://perma.cc/6NWL-SABL]; Standard Minimization Procedures, Exhibit A. In the Matter of the Application of the United States for an Order Authorizing Electronic Surveillance of a Non-United States Person Agent of a Foreign Power, No. [omitted] (FISA Ct. 1995), http://www.clearinghouse.net/chDocs/public/NS-DC-0008-0045.pdf [http://perma.cc/Z53S-6HHY]; Standard Minimization Procedures, Exhibit A. In the Matter of the Application of the United States for an Order Authorizing Electronic Surveillance of a United States Person Agent of a Foreign Power, No. [omitted] (FISA Ct. 1997), http://www.clearinghouse.net/chDocs/public/NS-DC-0008-0048.pdf [http://perma.cc/5SDS-X34B]; Submission of Amendment to Standard Minimization Procedures, In re Amendment to the Federal Bureau of Investigation's Standard Minimization Procedures for Electronic Surveillance and Physical Search, No. [omitted] (FISA Ct. 2006), http://www.clearinghouse.net/chDocs/public/NS-DC-0008-0046.pdf [http://perma.cc/8DSC-7JUG].

[54] For example, the 702 minimization procedures require: "A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing," that various prerequisites for retention are satisfied. US ATT'Y GEN. ERIC HOLDER, EXHIBIT B: MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 5 (Oct. 31, 2011) [hereinafter SECTION 702 NSA MINIMIZATION PROCEDURES], https://perma.cc/8LBM-CRRZ.

legalistic method of reasoned elaboration,[55] as they explain why the outcome they favor should be adopted by the official authorized to decide. As Mary Lawton, the Department of Justice lawyer who helped to draft FISA and was for several decades the most influential bureaucrat of intelligence legalism,[56] explained in 1993, "[i]mplicit in these requirements are certain formidable bureaucratic constraints: articulation, consideration, consensus and personal accountability," which together slow down and rationalize actions proposed.[57] Both "articulation" and "consideration" are characteristic of legalized decisions. Third, the procedures empower lawyers: they must be approved by the Attorney General, and therefore first by DOJ lawyers, prior to being offered to the FISA Court for its signoff.[58] Fourth, once approved, the procedures acquire the privileged status of federal court orders. Obedience becomes a compliance, rather than a policy, task for the NSA, subject to requirements of court disclosure and correction.[59] So if NSA fails—particularly if it fails systematically—the court might impose various consequences ranging from embarrassment for particular lawyers to withdrawing approval for a whole NSA program.[60] It is evident that these consequences are only loosely coupled with the substantive importance of the disregarded minimization feature; the FISA court has sometimes scolded

---

[55] HENRY M. HART, JR. & ALBERT M. SACKS, THE LEGAL PROCESS: BASIC PROBLEMS IN THE MAKING AND APPLICATION OF LAW 143 (William N. Eskridge, Jr. & Philip P. Frickey eds., 1994).

[56] *See* Piette & Radack, *supra* note 34, at 449; Ronald Sullivan, *Mary C. Lawton, 58: U.S. Official Shaped Intelligence Policies*, N.Y. TIMES (Oct. 30, 1993), http://www.nytimes.com/1993/10/30/obituaries/mary-c-lawton-58-us-official-shaped-intelligence-policies.html; MCGEE & DUFFY, MAIN JUSTICE, *supra* note 34.

[57] Mary Lawton, *Review and Accountability in the United States Intelligence Community*, OPTIMUM, Aug. 1993, p. 101. I agree with Lawton that these dynamics taken together are essentially bureaucratic, in addition to being legalistic; Lawton wrote that in the intelligence arena as in so many other policy spaces, "[b]ureaucracy itself is the prime control mechanism." *Id.*

[58] *See* 50 U.S.C. § 1801(h) (Title I FISA warrant for electronic surveillance); 50 U.S.C. § 1821(4) (Title III FISA warrant for physical search); 50 U.S.C. § 1861(g) (Title V business record/tangible things search); 50 U.S.C. § 1881a(e) (Title VII non-U.S. person abroad); 50 U.S.C. § 1881b(b)(1)(d) (Title VII U.S. person abroad probable cause order); 50 U.S.C. § 1881c(b)(4) (same, surveillance abroad).

[59] *See* FISA Court Rule 13, Correction of Misstatement or Omission; Disclosure of Non-Compliance, http://perma.cc/9DKM-KQ9A ("(b) Disclosure of Non-Compliance. If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made of . . . the facts and circumstances relevant to the non-compliance.").

[60] *See*, *e.g.*, In re Production of Tangible Things from [Redacted], No. BR 08-13, at 18 (FISA Ct. Mar. 2, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0011-0005.pdf [http://perma.cc/7PS6-5UGK] (suspending the government's ability to access telephony metadata collected pursuant its Section 215 authority except for the purpose of "ensuring data integrity and compliance with the Court's orders," and prohibiting the government from accessing any telephony metadata for the purpose of obtaining foreign intelligence unless the government requests such access from the Court on a case-by-case basis).

the government for noncompliance with minimization orders whose features it agrees to relax in the very same opinion.[61]

Post-September 11 amendments to and interpretations of FISA have vastly reduced the warrant-style individuation required for FISA-authorized surveillance. Under the FISA Amendments Act, the FISA Court now signs off on a massive program of targeted surveillance of foreigners—including when their communication is with an American—and on some smaller amount of targeted surveillance of U.S. persons abroad, without adjudicating the existence of probable cause for the targets.[62] And we now know that at least two bulk metadata programs—one examining a broad array of domestic internet communications, and the other focusing on an even larger share of domestic phone calls—have been deemed authorized by FISA without individuated suspicion of any party to the communications. Much of FISA surveillance,[63] that is, no longer resembles ordinary domestic criminal practice. Nonetheless the basic legalizing structure has remained intact: lawyers prepare, and judges approve, the proposed surveillance, and it is accompanied by court-ratified minimization procedures given the force of law.

C. Executive Order 12,333

Executive Order 12,333 (invariably referred to orally as, simply, "twelve triple three") is the "foundational" federal surveillance authority, applicable to all activities not otherwise regulated that touch or might touch U.S. person information.[64] Executive Order 12,333 has been amended three times since President Reagan issued it first in 1981, most recently and significantly in 2008, but it has retained its basic character.[65] As the

---

[61] In 2009, for example, Judge Reggie B. Walton allowed the government to continue using "defeat lists" in its handling of PR/TT metadata, even though those defeat lists "deviated, at least in part," from court-approved procedures. *See* Supplemental Order, No. PR/TT [Redacted], at 2 (FISA Ct. June 22, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0013-0001.pdf [http://perma.cc/9DFW-PJAB]. And in 2012, Judge Bates authorized "upstream" collection of internet communications under Section 702, even though he had previously held such collection to violate court orders. *See* Memorandum Opinion, No. PR/TT [Redacted] (FISA Ct. 2012), http://www.clearinghouse.net/chDocs/public/NS-DC-0057-0008.pdf [http://perma.cc/SKU6-QYAS].

[62] FISA Amendments Act, Pub. L. No. 110-261, 2436 Stat. 122 (2008); 50 U.S.C. § 1881a(e); 50 U.S.C. § 1881b(b)(1)(D); 50 U.S.C. § 1881c(b)(4) (minimization procedures for targeted searches abroad).

[63] For the terms of the internet metadata program, see Bates 2010 PR/TT Opinion, *supra* note 48; Kollar-Kotelly 2004 PR/TT Opinion, *supra* note 48, at 43–44. For the terms of the telephony metadata program, see the minimization procedures cited *supra* note 52.

[64] *See* NAT'L SEC. AGENCY, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS 2 (August 9, 2013), http://perma.cc/968K-YRXR.

[65] *See* Exec. Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981), *amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53594 (Aug. 27, 2004); and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008). For Exec. Order No. 12,333's predecessors, *see* Exec. Order No. 11,905, 41 Fed. Reg. 7703

organizing document for the nation's intelligence operations, it applies to the entire Intelligence Community (IC).[66] Individual IC elements then implement it via more focused guidelines, which are required to be signed by the Attorney General.[67] For the wide swathes of foreign intelligence surveillance that are not covered by FISA, regulation under Executive Order 12,333 occurs without judicial involvement. That is, where FISA does not apply, it is 12,333 that limits the collection, retention, use, and dissemination of U.S. person information, no matter what the method of surveillance—even if, for example, the communications are acquired from some foreign partner agency. The Executive Order explains that its "general principles . . . in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests."[68] For surveillance, its basic approach is two-fold: it insists on in-advance fully vetted written procedures, and it authorizes specific surveillance without court approval only if the Attorney General approves.

On the first point, surveillance, retention, use, and dissemination procedures must be approved in advance at a very high level within the administration; the Executive Order does not use the word "minimization" but the idea is the same. Such procedures are generally developed by the IC element involved, in consultation (in the most recent version) with the Office of the Director of National Intelligence, and then must be approved by the Attorney General.[69] Attorney General-approved procedures are required for:

- Coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States.[70]
- Intelligence collection, retention, and dissemination concerning U.S. persons.[71]
- Intelligence collection within the U.S. or directed against U.S. persons abroad.[72]

(Feb. 18, 1976) (Ford administration); Exec. Order No. 12036, 43 Fed. Rev. 3674 (Jan. 24, 1978) (Carter administration).

[66] Exec. Order No. 12,333 § 3.5(h) (listing the many agencies, departments, and offices that comprise the "Intelligence Community").

[67] *Id.* § 3.2.

[68] Exec. Order No. 12,333 § 2.2.

[69] *See* Exec. Order No. 12,333 § 2.3 (procedures governing collection, retention, dissemination of information concerning U.S. persons); § 2.4 (procedures governing collection within the U.S. or directed against U.S. persons abroad); § 2.9 (procedures governing IC element personnel surreptitious participation in an organization in the U.S.); § 3.2 (everything else in Part 2); *see also* § 2.3(j) (procedures on dissemination of SIGINT are to be developed by the DNI, in coordination with the Secretary of Defense; AG approval is required).

[70] *Id.* § 1.3(b)(20).

[71] *Id.* § 2.3 (developed by IC element, consultation with DNI).

[72] *Id.* § 2.4 (developed by IC element, consultation with DNI).

- How information possessed by all the executive agencies is provided to or accessed by the IC, and how that information may be used or shared.[73]
- Dissemination of Signals Intelligence (SIGINT).[74]

Evidently the Attorney General's disapproval on "constitutional or other legal grounds" is final. But the Attorney General is authorized to disapprove for other, non-legal reasons as well: "[W]here the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC [National Security Council]."[75]

What has emerged from this E.O. 12,333 process is a number of IC-element-specific "AG Guidelines." Once issued, these are bureaucratically difficult to change.[76] For the NSA, as part of the Department of Defense, the Executive Order 12,333 Attorney General guidelines were signed in 1982 as part of Department of Defense Directive 5240.1-R, and have not since been modified.[77] These are joined by other similarly amendment-resistant documents. At the NSA, such documents include a (now mostly de)classified annex governing NSA's role and procedures[78]; another document titled U.S. Signals Intelligence Directive 18 (generally referred to as USSID 18), which in turn has its own (de)classified annex and was apparently last updated in 2011[79]; and a formal policy document most recently issued in 2004, with yet another (de)classified annex.[80] Substantively, these documents together function like FISA minimization procedures, although they are laxer in several ways. Procedurally, however, they are very different. For FISA minimization, written justifications and

---

[73] *Id.* § 1.3(a)(2).

[74] *Id.* § 2.3(j) (developed by DNI, in coordination with the Defense Secretary).

[75] *Id.* § 3.2.

[76] For example, the AG Guidelines on Activities of DOD Intelligence Components that Affect United States Persons were signed in 1982. *See* DEP'T OF DEF., PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (DoD 5240.1-R, Dec. 1982) [hereinafter DOD DIRECTIVE 5240.1-R], http://perma.cc/X9QM-JR8E. For an account of the contentious process of reissuing one set of AG Guidelines, governing the National Counter-Terrorism Center, see Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53, 88–92 (2014), and sources cited.

[77] *See* DOD DIRECTIVE 5240.1-R, *supra* note 76.

[78] *See* NAT'L SEC. AGENCY & CENT. SEC. SERV., CLASSIFIED ANNEX TO DEPARTMENT OF DEFENSE PROCEDURES UNDER EXECUTIVE ORDER 12333, at 9 (ID 3199129, Mar. 11, 2004), *available at* https://perma.cc/EF7J-99CA.

[79] *See* USSID 18, *supra* note 49. The 1993 version is also available: 1993 USSID 18, *supra* note 49, at 26, along with its declassified Annex A, at 51–62.

[80] NAT'L SEC. AGENCY & CENT. SEC. SERV., NSA/CSS POLICY 1–23 (Mar. 11, 2004), https://perma.cc/4XSA-J2GX. The classified annex was apparently signed by Deputy Secretary of Defense William R. Taft and Attorney General Edwin Meese in April and May 1988, respectively. *See id.* at A-13.

explanations of each program are filed with the FISA Court and undergird each eventual court approval. Any change in the underlying processes might be material to the Court's approval, and therefore needs to be explained.[81] For E.O. 12,333 processes, the AG Guidelines are more freestanding; there is no subsequent formal implementation check. Thus even apart from the greater leeway allowed by the AG Guidelines, compared to FISA-approved minimization procedures, the result is substantially more operational freedom under 12,333 than under FISA.

In addition to its requirements of Attorney General-approved processes, Executive Order 12,333 "delegate[s]" to the Attorney General the authority "to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes," if the Attorney General finds "probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."[82] Under this provision, the Attorney General operates essentially like a warrant-granting magistrate, with operational control of the decision to initiate surveillance. (This requirement has been largely superseded by FISA Title VII, but it remains operative in some rare situations, and also in emergencies.[83]) While there is no judicial involvement, the process is very similar to a judicial one; the same lawyers who prepare FISA applications prepare a similar application for the Attorney General to approve (or reject).[84]

As a whole, then, notwithstanding the entire absence of court involvement, E.O. 12,333 is a key source of intelligence legalism. It is worth noting, too, that its text was one of the sites around which intelligence legalism was hotly contested. One of the Order's drafters, Richard Willard, recounted a few years later that when he arrived at the Department of Justice early in the Reagan administration, as Attorney General Smith's Counsel for Intelligence Policy, "holdover [career] officials in the intelligence

---

[81] *See, e.g.*, In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things From [Redacted], No. BR 09-06, at 4 (FISA Ct. June 22, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0013-0001.pdf [http://perma.cc/2295-SDDT] ("First, the government disclosed in its filings in Docket No. PR/TT [REDACTED] that NSA has generally failed to adhere to the special dissemination restrictions originally proposed by the government, repeatedly relied upon by the Court in authorizing the collection of the PR/TT metadata, and incorporated into the Court's orders as binding on NSA."). *See id.* at 2 ("As the government has acknowledged, its practices with regard to the creation and use of defeat lists for selectors deviated, at least in part, from the procedures governing the handling of PRITT metadata. It is important to note that the procedures at issue were devised by the government and incorporated into the Court's orders as binding upon the NSA at the government's suggestion. Had the government initially proposed procedures permitting defeat list practices such as those described in the [redacted] Response and the [redacted] Declaration, the Court likely would have found them reasonable and would have incorporated such procedures in its orders.").

[82] Exec. Order No. 12,333 § 2.5.

[83] IC Attorney Interview, *supra* note 15.

[84] *Id.*

community were busily drafting a new Executive order on intelligence activities that would virtually eliminate the legal oversight role of the Attorney General," because of the "enormous pent-up hostility in the intelligence community toward lawyers and legalistic restrictions."[85] This "attitude was not an invention of the Republican political appointees—who at that time were not yet that numerous—but permeated the career service."[86] It was his assignment, he explained, to mold Executive Order 12,333 into something more "balanced"[87]—that is, more pro-lawyer. He succeeded; E.O. 12,333 inserted the Attorney General deep into intelligence policy and even operations. This intervention marked a sharp change. Willard notes that in his time at the department,

> [t]he Attorney General was not a full member of the cabinet-level group that considered these [foreign intelligence and policy] matters but was only 'invited' to attend. It is my understanding that Attorney General Meese was later made a member of the group, but that even then some effort was made to insist that he was a member in his personal capacity and not as Attorney General. . . . As a consequence of the Attorney General's uncertain status in the process, his subordinates were generally excluded from working groups and subcabinet-level deliberations.[88]

In total, while the tendency is more extreme for FISA, each of the two foundational documents for foreign intelligence surveillance, FISA and Executive Order 12,333, has moved surveillance programs in legalistic directions, emphasizing rules and empowering lawyers.

The political theories underlying both of the 1970s intelligence reform strategies, disclosure and legalism, are obvious: disclosure serves accountability, and legalism serves the rule of law. But neither one directly seeks the appropriate balance between liberty and surveillance, however appropriateness is evaluated. One would therefore expect institutional arrangements premised on these two theories to serve disclosure and legalism, but to fail to prioritize, or even to weigh, individual's liberty interests when they are in tension with surveillance goals. This produces what I call the civil liberties gap. Part II explores whether this gap exists in practice, describing the NSA's existing compliance and oversight systems in some detail.

---

[85] Richard K. Willard, *Law and the National Security Decision-Making Process in the Reagan Administration*, 11 HOUS. J. INT'L L. 129, 130 (1988).
[86] *Id.*
[87] *Id*.
[88] Willard, *supra* note 86, at 131–32.

II. The NSA's Existing Compliance and Oversight Ecosystem

The NSA's General Counsel, Rajesh De, has described the NSA's total oversight apparatus as extremely thorough. "It is evident to me," De said in a speech in early 2013, "that I am the general counsel for one of the most highly regulated entities in the world."[89] With more exasperation, former NSA General Counsel Stewart Baker has argued that the whole system—an "army of second-guessers"—is too constraining:

> The judges of the FISA court have cleared law clerks who surely see themselves as counterweights to the government's lawyers. The government's lawyers themselves come not from the intelligence community but from a Justice Department office that sees itself as a check on the intelligence community and feels obligated to give the FISA court facts and arguments that it would not offer in an adversary hearing. There may be a dozen offices that think their job is to act as a check on the intelligence community's use of FISA: inspectors general, technical compliance officers, general counsel, intelligence community staffers, and more.[90]

Baker's estimated dozen offices was, in fact, the precise number:

- NSA Office of the Director of Compliance
- NSA Office of the General Counsel
- NSA Office of the Inspector General
- DOJ National Security Division, Office of Intelligence
- Assistant to the Secretary of Defense for Intelligence Oversight
- Intelligence Community Office of the Inspector General
- ODNI Civil Liberties Protection Office
- ODNI Office of the General Counsel
- ODNI Mission Integration Division (Office of the Deputy Director for Intelligence Integration)
- President's Intelligence Advisory Board, Intelligence Oversight Board
- FISA Court and FISA Court of Review
- Privacy and Civil Liberties Oversight Board

Add to that the newest office—NSA's Civil Liberties and Privacy Office.

---

[89] Rajesh De, Gen. Counsel, Nat'l Sec. Agency, Address at Georgetown Law School (Feb. 27, 2013), http://perma.cc/RP2N-9DB8.

[90] *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs: Hearing before the S. Comm. on the Judiciary*, 113th Cong. (July 29, 2013) (testimony of Stewart Baker, Partner, Steptoe & Johnson LLP), http://perma.cc/T4Z3-SQ5W.

In total, more than a few hundred people spend all or a substantial part of their work weeks on NSA compliance and oversight. This enormous staffing commitment itself demonstrates real commitment to abiding by the FISA and 12,333 rules. (In other topic areas, one might suspect that the commitment is to *being seen* to abide by the rules—but the IC's secrecy undercuts that cynical interpretation.) Nonetheless, inevitably, the agency is far from perfectly compliant. On occasion, compliance errors have been extremely widespread: In 2009, the government disclosed a series of significant compliance failures to the FISA Court affecting both the internet and telephony metadata programs. These included systemic failures to comply with the reasonable articulable suspicion standard, by use of less-strictly vetted alert lists and seed accounts; unauthorized sharing of unminimized query results with other agency personnel; and collection of fields of metadata beyond what was allowed by court order on nearly all the internet metadata records.[91] In addition, in 2011, the government reported that the "upstream" methods it was using to surveil American internet communications abroad were incapable of confining NSA access to only communications that met the standard for collection.[92] These were extremely significant failures, and they prompted some moderately robust responses—creation of the current NSA compliance office,[93] augmentation of the Justice Department oversight role,[94] and some stern (though for years secret) lectures by the FISA Court judges.[95]

---

[91] NAT'L SEC. AGENCY, BUSINESS RECORDS FISA NSA REVIEW 8, 16 (June 25, 2009) (Section 215 telephony metadata), http://www.clearinghouse.net/chDocs/public/NS-DC-0014-0001.pdf [http://perma.cc/JBB9-R569]; NAT'L SEC. AGENCY, PEN REGISTER/TRAP AND TRACE FISA NSA REVIEW (date redacted), http://www.clearinghouse.net/chDocs/public/NS-DC-0065-0002.pdf [http://perma.cc/336Q-6942].

[92] Memorandum Opinion, No. [Redacted], at 5 (FISA Ct. Oct. 3, 2011), http://www.clearinghouse.net/chDocs/public/NS-DC-0057-0002.pdf [http://perma.cc/US7V-7S6B].

[93] DeLong interview, *supra* note 15.

[94] *Compare* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 07-16, § 3(E) (FISA Ct. Oct. 18, 2007), http://www.clearinghouse.net/chDocs/public/NS-DC-0036-0001.pdf [http://perma.cc/CY7M-UF5K] (requiring the Justice Department to review a sample of the NSA's justifications for querying archived data at least once every ninety days), *and* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 08-08 § 3(E) (FISA Ct. Aug. 19, 2008), http://www.clearinghouse.net/chDocs/public/NS-DC-0040-0001.pdf [http://perma.cc/BNU9-Q879] (same, every sixty days), *with* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], BR 09-15, § 3(M), (N) (FISA Ct. Oct. 30, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0016-0002.pdf [http://perma.cc/ST3K-TWSY] (requiring the NSA's OGC to consult with NSD on all significant legal opinions that relate to authorizations by the FISA court), *and* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], BR 09-19, § 3(O), (P), (Q), (R) (FISA Ct. Dec. 16, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0053-0006.pdf [http://perma.cc/8JWM-AY34] (requiring the NSA's OGC to provide NSD with copies of

It is surely reasonable to expect better than these low points. But it would be unrealistic to demand either perfect compliance or perfect detection of noncompliance. Both are unattainable for an organization as complex as the NSA, governed by rulesets as complex as the Foreign Intelligence Surveillance Act, Executive Order 12,333, and their related procedural documents. Error, after all, has many causes. Sometimes the rules are misunderstood or miscommunicated.[96] Sometimes someone who understands the rules makes a mistake—enters a typo, for example,[97] or seeks approval later than the rules require.[98] Sometimes, one can imagine, systems fail—a computer algorithm that is supposed to distinguish among people with different statuses might miscategorize a new status, for example. And sometimes people try to defeat the rules.[99] In a system as massive and

---

all formal briefing and/or training materials used to brief and train NSA personnel in regard to the authorizations granted by the order).

[95] *See, e.g.*, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 09-13, at 4 (FISA Ct. Sept. 25, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0015-0002.pdf [http://perma.cc/S44V-72TP] (stating that "[t]he Court is deeply troubled" by compliance failures and ordering representatives of the NSA and NSD to appear before the court to explain); Order, No. PR/TT [Redacted], at 6 (FISA Ct. June 22, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0029-0001.pdf [http://perma.cc/7RGY-FML8] ("The Court is gravely concerned . . . that NSA analysts, cleared and otherwise, have generally not adhered to the dissemination restrictions proposed by the government, repeatedly relied upon by the Court in authorizing the collection of the PR/TT metadata, and incorporated into the Court's orders in this matter [redacted] as binding on NSA."); In re Production of Tangible Things From [Redacted], No. BR 08-13, at 5–8 (FISA Ct. Mar. 2, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0011-0005.pdf [http://perma.cc/KFT2-WZME] (stating that the government's justification for its non-compliance with the FISA Court's orders "strain[ed] credulity" and admonishing the government for its systemic compliance failures and "material misrepresentations" to the Court).

[96] *See, e.g.*, Bates 2010 PR/TT Opinion, *supra* note 48, at 10–11 (reporting unauthorized collection of data that "did not result from technical difficulty or malfunction, but rather from a failure of 'those NSA officials who understood in detail the requirements of the . . . [authorization] . . . to communication those requirements effectively to the [redacted] who were directly responsible' for the implementation").

[97] The Washington Post has reported that a "quality assurance" document (apparently not yet made public) says that in 2008, a typo in a program substituting the U.S. area code 202 for the international code 20-2 led to the collection of metadata about a "large number" of calls placed from Washington, D.C., instead of Cairo, Egypt. Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST, Aug. 15, 2013, http://perma.cc/9YNY-DGZ5. For more routine typo errors, *see, e.g.*, SID Oversight & Compliance, NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) Executive Summary, (May 3, 2012), http://perma.cc/59GV-GD6D.

[98] *See* ATT'Y GEN. & DIR. OF NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE AND SURVEILLANCE ACT 24 (Aug. 2013), http://perma.cc/9PG9-ST3T (describing reporting delays).

[99] *See* Letter from George Ellard, Inspector General, National Security Agency to Sen. Charles E. Grassley, Committee on the Judiciary (Sep. 11, 2013), http://www.scribd.com/doc/171424593/NSA-Surveillance-LOVEINT.

complicated as the NSA's signals intelligence program, even an extremely low rate of error can add up.[100] (Although because most of the information collected does not involve persons in the U.S. or Americans abroad, these errors frequently do not violate anyone's constitutional rights, under current doctrine.) Of course, each type of error can be reduced. But compliance errors are often hydraulic—pushing out errors in one place is likely to introduce at least some errors in another place.[101] The goal, then, is not zero errors, but rather, as the NSA's Director of Compliance puts it, to "assure compliance at a reasonable level."[102] NSA has not always achieved that goal—but it musters substantial effort to do so.

A. NSA Offices

Four offices at the NSA address civil liberties and privacy issues: the Office of the Director of Compliance, the Civil Liberties and Privacy Office, the Office of the Inspector General, and the Office of General Counsel. All but the second are compliance offices; the new civil liberties office is a policy development shop. I discuss them in turn.

1. NSA Compliance Office

The NSA has a central compliance office, the Office of the Director of Compliance, whose current (and founding) head, John DeLong, reports to the NSA's director. The compliance office grew out of several serious compliance problems exposed to the FISA Court in 2009,[103] and gained its statutory authority in 2010. It is assigned "responsib[ility] for the programs of compliance over mission activities."[104] Although the office is mentioned specifically only in some of the FISA minimization procedures, it seems to deal comprehensively not just with FISA-court supervised intelligence, but

---

[100] Consider the estimate that the NSA collects about 100 billion pieces of information from the internet monthly. *See* Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (June 11, 2013), http://perma.cc/HL5N-FV3S. The oft-cited "six sigma" business goal of no more than 3.4 defective parts per million, *see, e.g.*, MIKEL HARRY & RICHARD SCHROEDER, SIX SIGMA: THE BREAKTHROUGH MANAGEMENT STRATEGY REVOLUTIONIZING THE WORLD'S TOP CORPORATIONS (2000), would mean 340,000 monthly errors in that collection.

[101] For example, if a system guards against typos by offering only normalized inputs, via a pull-down menu, then that may greatly reduce the number of typing errors, but it simultaneously creates the opportunity for a more significant error if whoever inputs the menu options makes a mistake.

[102] Benjamin Wittes, *Lawfare Podcast Episode #53: Inside NSA, Part II – Wherein We Interview the Agency's Chief of Compliance, John DeLong*, LAWFARE (Dec. 17, 2013), http://perma.cc/PP7E-928Y.

[103] *See* text accompanying *supra* note 91.

[104] Intelligence Authorization Act for FY 2010, 50 U.S.C. § 3602(3) ("There is a Director of Compliance of the National Security Agency, who shall be appointed by the Director of the National Security Agency and who shall be responsible for the programs of compliance over mission activities of the National Security Agency.").

with all the procedures that are approved by the Attorney General under Executive Order 12,333—which means *all* the NSA's collection activities, as well as the retention, analysis, and dissemination of any U.S. person information. The NSA's compliance office is a member of the bureaucratic species I have labeled "Offices of Goodness"—it is an office within an operational agency that is: advisory rather than operational; tasked with furthering a particular value not otherwise primary for the agency in which it sits; and internal and dependent on its agency.[105] (I label that value with the placeholder, "Goodness," because the creator of the office obviously believes the particular value to be good.) For the NSA compliance office, the value that infuses its existence is, well, compliance: its mission is to facilitate NSA's compliance with constraints imposed upon the agency, detecting noncompliance consistently and rapidly.[106]

The compliance office has a staff of about 30. A much larger contingent of compliance staff—about another 270 employees—work within NSA's various operational units. The chain of command for these employees runs up through the heads of their units. But they report secondarily, via "as thick a dotted line as can be imagined," to the central compliance office.[107] The office was revamped and empowered in 2009, when many significant compliance problems came to light in FISA proceedings. Before that, there were fewer than 100 compliance staff throughout the NSA, including an Office of Oversight and Compliance housed deeper in the organizational chart, within the NSA's Foreign Intelligence Directorate. Currently, the compliance staff's tasks include developing procedures; working with engineers to hardwire the relevant requirements into computer systems; training; certifying procedures to the FISA Court; conducting both routine and broad compliance monitoring and reviews; and reviewing incidents of non-compliance. Thus NSA compliance staff work in an iterative way on non-compliance prevention, detection, and response, using both proactive and reactive strategies. DeLong explains that his office's current incarnation is modeled after corporate compliance offices, which frequently (particularly since the passage of the Sarbanes-Oxley Act) are placed outside the general counsel's office and with an office head who reports to the CEO. The work, DeLong says, is "organized functionally—for example, collecting, targeting, querying, sharing. That makes it easier to build compliance systems; it's good if those are somewhat uniform across activities. We're not stove-piped by authority, except for Section 215 [the telephony metadata program]."[108]

---

[105] Schlanger, *Offices of Goodness*, *supra* note 76.

[106] Email from John DeLong to author (Sept. 6, 2014) (on file with author).

[107] DeLong Interview, *supra* note 15.

[108] *Id.* For other sources in which DeLong has described his office, *see* Aliya Sternstein, *At NSA, Computers Sometimes Make the Policy Calls*, NEXTGOV (Aug. 20, 2012), http://perma.cc/7248-KKXC; Aliya Sternstein, *Compliance with Wiretap Law is Transparent, NSA Says*, NEXTGOV (Aug. 29, 2012), http://perma.cc/426M-VW34; Aliya Sternstein, *Eyes on Spies*, GOV'T EXEC. (Oct. 1, 2012) http://perma.cc/7LEF-SJ7X; Aliya Sternstein, *Meet the NSA Officer Charged With Balancing Surveillance and Civil Liberties*, NEXTGOV (Oct. 15, 2012), http://perma.cc/G5TN-UAE4; Julia Ziegler, *NSA Clears Up Misconceptions About Compliance*, FED. NEWS RADIO (Nov. 8, 2012),

The infrastructure that compliance staff use to accomplish this work is quite comprehensive. For example, under the applicable minimization rules, the NSA's systems used for FISA surveillance are built to create an audit trail. Database queries create a record that can later be reviewed to ensure that the person who provided the query had the right credentials and the required training, that the query itself met applicable rules, and so on. Compliance personnel are responsible for conducting periodic reviews that are thus enabled. Non-compliant uses are categorized, analyzed, and reported,[109] and sometimes new systematic safeguards are put in place as a result.[110]

Incident review systems supplement the periodic reviews. All NSA personnel are required to report any compliance mistakes or episodes of noncompliance with relevant court orders or other rules.[111] These reports then are distributed to the compliance office, as well as to the NSA Office of General Counsel (OGC) and NSA Office of the Inspector General (OIG).

---

http://perma.cc/PY6Y-B5NM; John M. DeLong, *For Agencies, the Intersection of Technology and Compliance Is Complex*, FEDTECH (Feb. 4, 2013), http://perma.cc/8BYM-C7TC; Benjamin Wittes, *Lawfare Podcast Episode #53: Inside NSA, Part II – Wherein We Interview the Agency's Chief of Compliance, John DeLong*, LAWFARE (Dec. 17, 2013), http://perma.cc/A3GF-AMZK; *NSA Compliance Director on Privacy Regulations*, DEFENSE NEWS, http://www.defensenews.com/VideoNetwork/2150661626001/NSA-Compliance-Director-on-Privacy-Regulations (last visited Aug. 16, 2014); *NSA Compliance Director on Keeping the Spies in* Line, DEFENSE NEWS, http://www.defensenews.com/VideoNetwork/2150661623001/NSA-Compliance-Director-on-Keeping-the-Spies-In-Line (last visited Aug. 16, 2014).

[109] For a still-classified example, *see NSA Report on Privacy Violations in the First Quarter of 2012*, http://perma.cc/484V-A84Q. A few 702 compliance reports have been declassified, but all but the last are too heavily redacted to provide much information. *See Semiannual Assessment of Compliance with FISA Amendments Act Procedures and Guidelines, Submitted by the Attorney General and the Director of National Intelligence* (March 2009) (reporting period: Sept. 4, 2008–Nov. 30, 2008), https://perma.cc/HY5F-6PB9; *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence* (Dec. 2009) (reporting period: Dec. 1, 2008–May 31, 2009), https://perma.cc/8LHZ-XMVE; *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director Of National Intelligence* (May 2010) (reporting period: June 1, 2009–Nov. 30, 2009), https://perma.cc/QNN7-DAHD; *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Submitted by the Attorney General and the Director of National Intelligence (Aug. 2013) (reporting period: June 1, 2012–Nov. 2012), http://perma.cc/RS3R-FKQV.

[110] Delong Interview, *supra* note 15.

[111] DOD DIRECTIVE 5240.1-R, *supra* note 76, at C15.3.1.1 ("Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO)."); *id.* at C15.2.1 ("The term 'questionable activity' . . . refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive order or Presidential directive, including E.O. 12,333 . . . or applicable DoD policy, including this Regulation.").

For the 702 program, NSA OGC also forwards each incident report to the Department of Justice and to the Office of the Director of National Intelligence (ODNI).[112] All FISA compliance errors are to be disclosed to the FISA judge who approved the relevant order.[113] For non-FISA matters, where the NSA OGC "ha[s] reason to believe" that the incident "may be unlawful or contrary to executive order or presidential directive," further reports go, via ODNI, to the President's Intelligence Oversight Board.[114] Each of these incidents requires follow up within NSA: compliance staff share the obligation to follow up with the Office of the Inspector General.

Overall, the compliance office performs a blend of compliance oversight and what DeLong calls "rules coaching":

> A compliance officer and the compliance organization is there really as more of a rules coach, if you will . . . not deciding what the rules are—that's the lawyers and policy folks—not building technology, not doing operations, but getting in there, rolling our sleeves up, right? Really kind of on the field . . . not as a referee, not . . . up in the stands, but as . . . a rules coach.[115]

2. NSA Office of Civil Liberties and Privacy

Within a few weeks of the Snowden disclosures, the President announced that the NSA would "put in place a full-time civil liberties and privacy officer."[116] This particular bureaucratic structure is one that has developed over the past decade, during which several IC components and agencies that include such components—ODNI, CIA, DoD, DHS, DOJ, and others—have added Privacy and Civil Liberties Offices.[117] Apparently the

---

[112] ATT'Y GEN. & DIR. OF NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE AND SURVEILLANCE ACT A-7 (Aug. 2013) [hereinafter SEMIANNUAL ASSESSMENT OF COMPLIANCE PROCEDURES], http://perma.cc/M7PN-BFX5.

[113] *See* FISA Court Rule 13, http://perma.cc/ADY8-PGEH.

[114] *See* Exec. Order No. 12,333 § 1.6(c); Exec. Order No. 13,462 §§ 6(b)(i)(a), 7. (Note that Exec. Order No. 13,462 refers to § 1.7 of Exec. Order No. 12,333, which was subsequently renumbered.)

[115] *NSA Compliance Director on Privacy Regulations*, DEFENSE NEWS, http://www.defensenews.com/VideoNetwork/2150661626001/NSA-Compliance-Director-on-Privacy-Regulations (last visited Aug. 16, 2014).

[116] Press Release, President Barack Obama, Remarks by the President in a Press Conference (Aug. 9, 2013), http://perma.cc/R8AZ-EP76.

[117] *See* 42 U.S.C. § 2000ee-1(a); *see also* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, §§ 1011, 1061, 118 Stat. 3638, 3658-59, 3688. These positions are variously constituted as career or political appointments. In some organizations they report directly to the agency head, but in others they are substantially lower down in the organization chart. *See, e.g.*, Memorandum from the Office Sec'y of Def., U.S. Dep't of Def., *Results of the office of the Secretary of Defense Organizational Review*, OSD 014014-13 (Dec. 4, 2013), https://perma.cc/SD3H-U9EL; *Biography of Michael L. Rhodes – Director of Administration and Management (OSD)*, U.S. DEP'T OF DEF.,

introduction of a civil liberties and privacy officer was not forced upon the NSA; officials there sponsored and embraced the idea.[118] The job announcement went up in September 2013,[119] and the new NSA Civil Liberties and Privacy Officer, Rebecca Richards, began work four months later.[120]

The role was clearly designed to be a policy job—helping to develop the rules, not merely promoting compliance with them. The job posting included the following specific duties:

> b. As the senior architect for CL/P [civil liberties/privacy], ensure that protections are addressed as part of all internal strategic decision processes related to the agency's operations, key relationships, tradecraft, technologies, resources or policies. . . .
> e. Manage CL/P policy, and advise on related assessment and compliance programs. . . .
> h. Provide CL/P reviews and assessments as required of the NSA support to the U.S. Cyber Command.[121]

As one might expect given the novelty of the position at the NSA, Richards is still working out her office's role and procedures. She reports that the office, which currently has six other employees, has three main functions: providing advice to NSA's Director, developing civil liberties and privacy protections, and enhancing public transparency. Her priority, she says, is to "build in" evaluation of civil liberties and privacy interests as part of the NSA's mission processes. The compliance office will continue to manage compliance, and the Office of the General Counsel, legal analysis. But the new Civil Liberties and Privacy Office should be, she says, "the focal point at NSA for assessing mission-related civil liberties and privacy risks, helping with mitigation strategies, and communicating as appropriate with the public." The office brings "a different perspective" into NSA conversations in furtherance of the goal of "reduc[ing] the impact of surveillance on ordinary people." The job is both procedural and substantive: "My job is to bring together mission folks, and others to ask, systematically, what are we doing and why, and whether the privacy and civil liberties impacts are worth the operational gain." What's new about her office, she says, is that "we are taking a more comprehensive civil liberties and privacy risk assessment process that allows decision-makers to consider a broader set

---

http://perma.cc/FFE4-34MX (last visited Nov. 16, 2014); Defense Privacy and Civil Liberties Office: Organizational Structure, U.S. DEP'T OF DEF., http://perma.cc/6CRR-CEQS (last visited Nov. 16, 2014).

[118] DeLong Interview, *supra* note 15.

[119] Edward Moyer, *NSA job post for 'Civil Liberties & Privacy Officer' goes live*, CNET (Sept. 20, 2013, 3:28 PM), http://perma.cc/W775-SESB.

[120] Press Release, National Security Agency, NSA Announces New Civil Liberties and Privacy Officer (Jan. 29, 2014), http://perma.cc/2B2Z-W9TE.

[121] Moyer, *supra* note 119.

of civil liberties and privacy values beyond the Constitutional considerations, the laws and judicial interpretation." In addition, Richards does substantial outreach, spending "quite a bit of [her] time engaging with the various privacy groups to better understand their concerns and share that within NSA."[122]

Richards points to "new presidential direction" as part of the impetus for change that underlies her new role. She anticipates that sometimes the result will be a decision by the NSA "not to pursue certain mission activities." Other times the advice may not be to avoid an activity, but rather "protections that mitigate civil liberties and privacy impacts."[123]

So far, the visible output of the new office has been two unclassified papers, one submitted to the Privacy and Civil Liberties Oversight Board (PCLOB), summarizing surveillance under FISA Section 702 and the various policies that apply to it,[124] and one about non-bulk collection under 12,333.[125] Richards received some criticism from observers who found the papers too positive; the surveillance go-to blog Emptywheel described the first one as "propaganda" that "doesn't so much read as an independent statement on the privacy assessment of the woman at the NSA mandated with overseeing it, but rather a highly scripted press release."[126] Others have disagreed. For example, one commentator called the 702 paper "remarkable for its transparency." [127] Richards defends these types of documents as appropriate steps towards transparency, pointing out that the NSA has never produced such reports in the past. She emphasizes that she does not conceptualize public criticism of the NSA as part of her new office's role. The idea, rather, is to advocate internally for and implement civil liberties and privacy protections, and then advise the public what those protections are. The IG's office, the PCLOB, and other entities can deliver public criticism.[128]

---

[122] Richards Interview, *supra* note 15.

[123] *Id.*

[124] NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE, REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 (April 16, 2014), http://perma.cc/4785-WRJ2.

[125] NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT, NSA'S CIVIL LIBERTIES AND PRIVACY PROTECTIONS FOR TARGETED SIGINT ACTIVITIES UNDER EXECUTIVE ORDER 12333 (Oct. 7, 2014), https://perma.cc/WZ5R-SKAP.

[126] *NSA's New "Privacy Officer" Releases Her First Propaganda*, EMPTYWHEEL (Apr. 21, 2014), http://perma.cc/D6VL-RYUE.

[127] John Kropf, *Why the New NSA Section 702 Report Is Remarkable*, PRIVACY PERSPECTIVES (Apr. 25, 2014), https://perma.cc/US7W-5T5R.

[128] Richards Interview, *supra* note 15.

3. NSA Office of Inspector General

The work of the NSA Office of Inspector General is authorized or required by statute,[129] internal Department of Defense directives,[130] and the FISA minimization rules themselves. IG staff play no role in NSA compliance development work—the engineering, procedure development, and the like. But their work with respect to audits and incident investigation complements that of the compliance office—absent the "rules coach" approach. Instead, the IG's stance is more independent—such independence is, for this as for other federal IGs,[131] the basic assignment.[132] This kind of task-duplication but not role-duplication obtains more generally, too. IG inspections related to compliance matters are carried out in tandem, but not jointly, with either the compliance office or the Office of General Counsel, so that each is done by both ordinary agency and independent staff. When the IG investigates potentially criminal misconduct, however, its jurisdiction within NSA is generally exclusive.

---

[129] *See* 5 U.S.C.A. App. 3 (generally, and especially § 8H); *see also* 50 U.S.C. § 3033 (establishing the Inspector General for the Intelligence Community).

[130] DOD 5240.1-R instructs agency personnel to report "questionable activity" to the IG, and instructs the IG to seek out such activity even if not reported, and to promptly investigate. DOD DIRECTIVE 5240.1-R, *supra* note 76, at C15.3.1-.2. The results are then passed along in quarterly reports to the Assistant to the Secretary of Defense for Intelligence Oversight. *Id.* at C15.3.1-3.3. In addition, USSID 18 requires the IG to "[c]onduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID," and "[e]stablish procedures for reporting by NSA/CSS signals intelligence elements of their activities and practices for oversight purposes." USSID 18, *supra* note 49, §§ 8.1(a)-(b). It requires the IG (along with the NSA's Director and General Counsel) to report regularly on compliance matters to the President's Intelligence Oversight Board, *id.* § 8.2(f) and annually to the NSA's Director, *id.* § 8.1(c). And OIG staff meet with Department of Justice NSD lawyers about telephony metadata every quarter "to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders." In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 11-57, § F(v) (FISA Ct. Apr. 13, 2011) [hereinafter 2011 Section 215 Minimization Order], http://www.clearinghouse.net/chDocs/public/NS-DC-0046-0001.pdf [http://perma.cc/2EVC-CGN2]. Occasionally, the NSA OIG is also assigned a much more precise task. For example, for surveillance under E.O. 12,333, the OIG annually reviews NSA's use of term searching. USSID 18, *supra* note 49, § 5.2 ("Annual Review by the Signals Intelligence Director"); § 5.2(c) ("A copy of the results of the review will be provided to the Inspector General (IG) and the GC.").

[131] *See* Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655, 1744 (2006). The overall framework for Offices of Inspectors General is set by the Inspector General Act of 1978, Pub. L. No. 95–452, 92 Stat. 1101. It establishes that Inspectors General, whether appointed by the President and confirmed by the Senate, or "administratively appointed" by their agency head, have investigative and congressional reporting obligations. In 2006, Congress passed technical legislation to bolster the independence and access of the NSA and other national security IGs. *See* 5 U.S.C.A. App. 3 § 8G(a)(2); Pat Roberts, Intelligence Authorization Act for Fiscal Year 2007, To Accompany S. 3237, S.R. No. 109-259, §433, at 29 (2006), http://perma.cc/VN9B-JYBV.

[132] *See* 5 U.S.C.A. App. 3 § 8H.

Others have written extensively about Intelligence Community IG's Offices,[133] examining the parameters of their independence and efficacy. IG's Offices clearly vary in their aggressiveness, expertise, and influence.[134] I have little to add here, except to note that IG's offices are focused in nearly all their activity on whether their agencies have followed applicable rules—and *not* on evaluation of those rules' content. Indeed, the joining of misconduct investigations and other compliance reviews in the single entity of an IG's office must tend to reinforce this mindset. The current NSA Inspector General, George Ellard, confirmed in a rare public appearance that he considers his oversight to cover the legality, not the wisdom, of NSA operations. Asked what he would have done if Snowden had come to him with complaints about the telephone metadata program, Ellard explained that he had an obligation to independently assess the program's constitutionality. And discussing the efficacy of existing oversight systems, he emphasized the rarity of intentional law violations. Not once, however, did he hint that the NSA IG's Office might ever independently assess program justifications or successes, to evaluate whether surveillance's costs to liberty were worthwhile.[135]

4. NSA Office of General Counsel

NSA's Office of General Counsel is the heart of intelligence legalism at NSA. Its role is more complex than that of the offices described above. Like the compliance office and the IG's office, NSA OGC lawyers promote compliance with the applicable rules, including by working on the

---

[133] For discussion of Inspectors General, see Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013); Ryan M. Check & Afsheen J. Radsan, *One Lantern in the Darkest Night: The CIA's Inspector General*, 4 J. NAT'L SEC. L. & POL'Y 247 (2010); Kathryn E. Newcomer, *The Changing Nature of Accountability: The Role of Inspector General in Federal Agencies*, 58 PUB. ADMIN. REV. 129 (1998); Michael R. Bromwich, *Running Special Investigations: The Inspector General Model*, 86 GEO. L.J. 2027 (1998); PAUL C. LIGHT, MONITORING GOVERNMENT: INSPECTORS GENERAL AND THE SEARCH FOR ACCOUNTABILITY (1993); INSPECTORS GENERAL: A NEW FORCE IN EVALUATION (Michael Hendricks et al. eds., 1990); Margaret J. Gates & Marjorie F. Knowles, *The Inspector General Act in the Federal Government: A New Approach to Accountability*, 36 ALA. L. REV. 473 (1984); CARMEN R. APAZA, INTEGRITY AND ACCOUNTABILITY IN GOVERNMENT: HOMELAND SECURITY AND THE INSPECTOR GENERAL (2011); MARK H. MOORE & MARGARET JANE GATES, INSPECTORS-GENERAL: JUNKYARD DOGS OR MAN'S BEST FRIEND (1986).

[134] It may or may not be a comment on the perceived aggressiveness of the NSA IG's Office that the ODNI General Counsel worked in 2007 with congressional staffers to ensure that draft legislation did not empower the DOJ IG's office to "review NSA's compliance with acquisition and minimization procedures," but rather left that task to NSA's own IG. Email from Brett Gerry (Friday, October 12, 2007 2:40 PM), https://www.eff.org/files/filenode/foia_C0705278/20091109_oip_group6.pdf. I was alerted to this document by *The EFF FOIA Working Thread*, EMPTYWHEEL (Nov. 12, 2009), http://perma.cc/RUE4-QMAA.

[135] Symposium, *National Security Law & Policy Journal Symposium*, GEORGETOWN LAW (Feb. 25, 2014, 9:00 AM), http://perma.cc/DJF5-LF4M (Panel III, A New Paradigm of Leaking). See especially the discussions starting at hour 4:23, 4:40, and 5:02. I thank Steve Vladeck for bringing this panel to my attention.

development of compliance training and sharing various reporting obligations with the IG's office staff. But OGC lawyers add to the mix rule interpretation: they help to determine what the rules mean by giving legal advice and participating in litigation.

Like the compliance office and the IG's office, NSA's OGC has responsibility—usually but not always partial responsibility—for various oversight tasks.[136] Under the telephony metadata minimization procedures, for example, NSA OGC staff are required to meet with staff from the compliance office and the Department of Justice National Security Division (NSD), described in the next section, to "assess[] compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired."[137] Along with NSD, NSA OGC must also "review a sample of the justifications for [Reasonable Articulable Suspicion] RAS approvals for selection terms used to query the BR metadata."[138] And when term searching is used on communications surveilled under Executive Order 12,333, a review of those terms is required to be performed by operational supervisors, with "[a] copy of the results of the review . . . provided to the Inspector General (IG) and the GC,"[139] for their further review. More generally, under the DOD rules implementing Executive Order 12,333, the General Counsel (along with the Inspector General) is required to submit quarterly reports to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), setting out "significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system."[140] Under the same DOD Directive, the OGC and OIG oversight roles extend to compliance problems as well: a quarterly report is required "describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive order or Presidential directive, or applicable DOD policy; and actions taken with respect to such activities."[141]

In fact, observers report that NSA's Office of General Counsel plays very much the lead role within the agency with respect to *non*-compliance. "As a practical matter," one senior IC lawyer says, "non-compliance identification and remediation seem to be driven by the lawyers."[142] When

---

[136] *See, e.g.*, USSID 18, *supra* note 49, Annex A, App. 1, Sec. 3(g)(2) (Title I minimization procedures) ("When any person involved in collection or processing of an electronic surveillance being conducted pursuant to the Act becomes aware of information tending to indicate a material change in the status or location of a target, the person shall immediately ensure that the NSA's Office of General Counsel is also made aware of such information.").

[137] 2011 Section 215 Minimization Order, *supra* note 130, § F(iv), at 15.

[138] *Id*. § F(vi), at 16.

[139] USSID 18, *supra* note 49, § 5.2(c).

[140] DOD DIRECTIVE 5240.1-R, *supra* note 76, at C15.3.3.2.

[141] *Id*.

[142] IC Attorney Interview, *supra* note 15.

an issue of potential non-compliance arises, "it's really the lawyers driving the questions in terms of the factual development, the analysis in terms of whether it's legal, and the subsequent reporting." Even lawyers describe this as perhaps an historical artifact, rather than an ideal organizational arrangement: "Maybe once you have a mature robust compliance structure, it shouldn't be driven by the lawyers. But that's definitely how it works" at the NSA.[143]

By this point, it should be clear that many NSA employees are assigned to compliance work—promoting rule-following and detecting and preventing rule violations. What NSA OGC adds more uniquely is application of law to fact and rule interpretation when there is ambiguity. This kind of legal advice is the most basic output of an agency law office. Like, I imagine, most federal Offices of General Counsel, NSA OGC provides both formal and informal advice. For example, many NSA training slides include references to day-to-day informal legal advice available from OGC lawyers: "Questions? Office of General Counsel (Operations/Intel Law) NSOC [National Security Operations Center] has an attorney on call 24/7!" And USSID 18 formally assigns NSA's OGC the role of "[r]eview[ing] and assess[ing] for legal implications as requested by the DIRNSA/CSS [the NSA Director], Deputy Director, IQ, Signals Intelligence Director, or their designees, all new major requirements and internally generated USSS [U.S. SIGINT System] activities."[144] In fact, the agency's General Counsel is designated to be the final decisionmaker on certain questions framed as legal. For example, under the NSA's metadata programs, OGC reviews any "RAS" (reasonable articulable suspicion) determination relating to a U.S. person to ensure that it is not based solely on First-Amendment protected activity.[145] Similarly, it is OGC that reviews and decides the appropriateness of proposed disseminations of U.S. person information that might infringe on attorney/client or doctor/patient privilege, or that involves criminal activity or judicial proceedings in the United States.[146] In addition, much advice is provided as part of litigation support, a key avenue by which agency lawyers exercise influence. As in many agencies, NSA litigation is both affirmative (the FISA docket) and defensive,[147] and OGC lawyers are important gatekeepers not only for formal litigation but also for its executive analogue under Executive Order

---

[143] *Id.*

[144] USSID 18, *supra* note 49, § 8.2(d); *see also* § 8.2(a) ("Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities."); (c) ("Advise the IG in inspections and oversight of USSS activities."); § 8.2(e) ("Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.").

[145] For Section 215, see 2011 Section 215 Minimization Order, *supra* note 130, at § 1(b)(3)(C)(i).

[146] USSID 18, *supra* note 49, § 7.4.

[147] *See, e.g.*, Bates 2010 PR/TT Opinion, *supra* note 48; Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d. 724 (S.D.N.Y. 2013).

12,333, even though the Department of Justice has closer to final authority for FISA matters, and final authority for non-FISA matters.[148]

One key question about all this legal advice is whether it is ever constraining—whether the lawyers ever tell their clients no. NSA's lawyers do sometimes advise their clients/colleagues not to do specific things. One released training document, for example, advises analysts not to use certain search techniques, cautioning: "Do Not: Wildcard domains. Wildcard user names. Wildcard across domains."[149] One would expect agency counsel to say no with relative ease where the rules are clear and when those rules govern *how* and not *whether* a particular activity can occur. It is crucial to remember, however, that agency lawyer advice-giving is not adjudication and agency lawyers are not judges. The judicial ideal of even-handedness is not, even theoretically, applicable. Rather, the goal of legal advice for lawyers within the Intelligence Community, as with any organization's lawyers, is to assist the client. To quote the same senior IC lawyer, "you're hoping to get done what your client wants to get done, so there's a tendency to try to find the most room to get that done."[150] Or, in the less careful words of a former NSA chief analyst, "Look, NSA has platoons of lawyers and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole."[151] Unsurprisingly, then, some training slides that say no also include work-arounds—methods for achieving various searching or analytic goals that are *not* covered by the stricter FISA rules.[152]

But what about when the issues are less clear, and the advice is not *how* but *whether* to undertake some proposed action? Here, one should expect lawyers to offer even less constraint on their agencies. Consider a 2005 speech to the NSA's lawyers and their colleagues, by then-Deputy

---

[148] Sometimes the gatekeeping function is implicit. For example, USSID 18 specifies that the office should "[p]repare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures." USSID 18, *supra* note 49, § 8.2(b); *see also, e.g.*, DOD DIRECTIVE 5240.1-R, *supra* note 76, at C5.5.2.1.4. The natural (though not quite inevitable) result is that the General Counsel and his staff gain decision-making authority about which applications can move forward and which cannot. Other times, the gatekeeping function is spelled out. For example, the telephony metadata minimization procedures specify "prior to implementation of any new or modified automated query processes, such new or modified processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court." 2011 Section 215 Minimization Order, *supra* note 130, § F(vii), at 16.

[149] *See, e.g.*, NSA Cryptological School Course on Legal, Compliance, and Minimization Procedures (Aug. 1, 2009), http://perma.cc/L7MM-MX63 ("Do Not: Wildcard domains. Wildcard user names. Wildcard across domains.").

[150] IC Attorney Interview, *supra* note 15.

[151] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://perma.cc/BM7S-9FTF.

[152] Module 4, OVSC1205 Special Training on FISA, Version 28, at 17, 22 (Oct. 17, 2011), http://perma.cc/ZFD3-66AR.

Attorney General James Comey, in which he praised the NSA's lawyers as "custodian[s] of our constitution and the rule of law." Their "commitment to the rule of law," he explained, not only served American constitutionalism, but would also protect their agency from "the damage that comes from the pendulum swings of American public life, the pendulum swings that pushed us so far backwards in the late 1970s, again in the late 1980s." And, he said, their training as lawyers equipped them to develop and act on the understanding that "in the long run, intelligence under law is the only sustainable intelligence in the country." Comey's speech was evidently intended to stiffen his audience members' backbones; he exhorted them to say "'yes' when it can be," but "'no' when it must be." That language ("can" versus "must") favors "yes" over "no," of course. As in all representation settings, lawyers' professional commitments to the rule of law are coupled with their professional commitments to serve their clients' interests and projects.[153] Agency lawyers are unlikely to lie down on the railroad tracks to stop an agency train; they are far more inclined by training, career incentives, and professional norms, to construct arguments to justify the train's forward motion. And when at least some of the lawyers' colleagues are arguing that lives are at stake, saying no is particularly hard. To quote Comey again:

> It can be hard . . . because the stakes couldn't be higher. Hard because we are likely to hear the words: "If we don't do this, people will die." You can all supply your own this: "If we don't collect this type of information," or "If we don't use this technique," or "If we don't extend this authority." It is extraordinarily difficult to be the attorney standing in front of the freight train that is the need for "this." Because we don't want people to die. In fact, we have chosen to devote our lives to institutions whose sworn duty it is to prevent that, whose sworn duty it is to protect our country, our fellow Americans.[154]

A recent book by long-time CIA career lawyer (and, at one time, its acting General Counsel) John Rizzo encapsulates agency lawyers' position in its title: *Company Man*.[155] Rizzo's book, in which he simultaneously touts his own influence and his disinclination to use it, demonstrates several times over that intelligence lawyers are not likely to shut down programs dear to their clients. Writing, for example, about the illegal arms-for-hostages deal of Iran-Contra, Rizzo ruminates:

---

[153] *See, e.g.*, Charles Fried, *The Lawyer as Friend: The Moral Foundations of the Lawyer-Client Relation*, 85 YALE L.J. 1060 (1976); Stephen L. Pepper, *The Lawyer's Amoral Ethical Role: A Defense, A Problem, and Some Possibilities*, 11 AM. BAR FOUND. RES. J. 613 (1986).

[154] Comey, *supra* note 4.

[155] JOHN RIZZO, COMPANY MAN: THIRTY YEARS OF CONTROVERSY AND CRISIS IN THE CIA (2014).

> Perhaps things might have turned out differently if I had been given a say—for a time I was pleased to believe that—but the truth is they probably wouldn't have. The arms-for-hostages initiative was conceived and approved at the highest levels [and] in all likelihood I would have gone along, whatever my private misgivings might have been."[156]

Similarly, describing his part in signing off on "enhanced interrogation techniques" for captured terrorists, such as waterboarding, Rizzo states, "My experience gave me confidence that I could squelch at least the more aggressive proposed EITs [enhanced interrogation techniques], then and there, if I wanted to. It would have been a relatively easy thing to do, actually."[157] But Rizzo did not say no.

The public record does not allow comprehensive assessment of how high stakes legal advice has played out at the NSA. When asked not simply about application of rules within a program but about that program's permissibility altogether, it may be that one of NSA's General Counsels has said no, counseling the agency that it cannot undertake some program or activity to which NSA's Director or even more senior executive officials are committed. No such situations, however, have yet been disclosed. Rather, we have abundant evidence that NSA's lawyers are—as any organization's lawyers would likely be—professionally disposed against even plausible—though not iron-clad—legal challenges to their agency's authority. Recounting a day spent at the NSA, Steve Vladeck summarizes:

> [W]hat became increasingly clear as the day wore on is how unable the NSA is to appreciate the possibility that the rules themselves might be legally or constitutionally invalid. . . . Several of the officials bristled at any suggestion that the agency was actually exceeding its legal authority, even though there are good arguments on both statutory and constitutional grounds. We heard several times how frivolous the Fourth Amendment challenge to the metadata program must be. Yet, just four days after the visit, the district court in Washington issued a decision to the contrary.[158]

Probably, agency counsel lack the perspectival distance—and perhaps the stature—to veto important agency initiatives. We saw this dynamic in effect in the case of the brief 2004 shutdown of the "President's Surveillance Program" internet metadata collection. "NSA leadership, including OGC lawyers and the IG," had ratified the program as lawful based on the

---

[156] *Id*. at 128.

[157] *Id*. at 186.

[158] Stephen Vladeck, *My Day at the NSA: A PR Campaign for Secret Surveillance Programs*, MSNBC (Dec. 17, 2013), http://perma.cc/K3NM-KL6C.

stretched argument that "NSA did not actually 'acquire' communications until specific communications were selected" for analysis—that is, until communications "hit" on a search.[159] It was not NSA career lawyers or their political appointee boss, NSA General Counsel Robert Dietz,[160] who triggered the hospital-bed confrontation that led to the temporary shutdown, or who then led the way in persuading the FISA Court to allow this aspect of the President's Surveillance Program to be squeezed into FISA's Pen Register title.[161] The lawyers who first concluded that the program was illegal as constituted and then stood up to the President's counsel and Chief of Staff, and to Vice President Cheney and his counsel,[162] were higher-ranked, and worked at the more prestigious and bureaucratically separate Department of Justice Office of Legal Counsel,[163] where they were, in the end, supported by Deputy Attorney General James Comey, himself supported by the ill Attorney General John Ashcroft.

Putting aside high ranking Department of Justice lawyers, federal agency counsel typically lack the stature to flout the views of White House lawyers. And this may be particularly true for the NSA. Consider that when the NSA's General Counsel asked to see the first Office of Legal Counsel opinion ratifying the initial internet metadata program, the White House declined even to share it.[164] Even if NSA's lawyers, up to the General Counsel, wanted to find a given program unlawful, their legal opinion could be less influential than that of similarly placed counsel in other agencies, because the extremely comprehensive involvement of the Department of Justice's National Security Division depresses the agency lawyers' ultimate authority: NSA OGC functions as something of a junior partner to the NSD and its leadership. (On the other hand, NSA OGC's position as the NSA's ordinary point of contact with the Department of Justice, following the bureaucratic logic that likes should link to like, simultaneously augments the bureaucratic influence of NSA OGC in more run-of-the-mill situations.)

And so it seems most likely that NSA OGC's advice in legally ambiguous, high-stakes situations poses little obstacle to proposed agency activities. The practical reality that lawyers are not very constraining goes hand in glove with their growing numbers and dockets inside intelligence

---

[159] NSA Draft IG Report, *supra* note 1, at 38. This argument is attractive enough to intelligence operators that it rears its head periodically, notwithstanding its implausibility as a matter of text and policy. In *Klayman*, for example, the district court rejected the argument, proffered by the government, that "'the mere collection of Plaintiffs' telephony metadata . . . without review of the data pursuant to a query' cannot be considered a search 'because the Government's acquisition of an item without examining its contents 'does not compromise the interest in preserving the privacy of its contents.'" Klayman v. Obama, 957 F. Supp. 2d. 1, 29 n.40 (D.D.C. 2013) (quoting Govt.'s Opp'n at 49 n.33).

[160] *See*, *e.g.*, BAMFORD, THE SHADOW FACTORY, *supra* note 1, at 116.

[161] NSA Draft IG Report, *supra* note 1, at 40–42.

[162] BAMFORD, THE SHADOW FACTORY, *supra* note 1, at 280–86.

[163] *See* Jack L. Goldsmith, III, *Memorandum for the Attorney General: Review of the Legality of the STELLAR WIND Program* (May 6, 2005), http://perma.cc/X8D4-7LXA.

[164] 2009 NSA Draft IG Report, *supra* note 1, at 21.

agencies. In an article two decades ago, intelligence official Dorian Greene repeated Richard Willard's earlier description of the IC's negative views of lawyers—"enormous pent-up hostility in the intelligence community toward lawyers and legalistic restrictions."[165] Greene attested in 1994 that "ten years later this general attitude has not shown any remarkable change."[166] Switching to the perspective of the lawyers themselves, he described theirs as an "uncomfortable position," because "[s]imultaneously the lawyer is both a servant for the [intelligence] community during the course of its relations with the remainder of the federal government and an oversight functionary within the community itself."[167] But over the past two decades, and particularly the latter of them, much has shifted. Lawyers—with their interpretive skills combined with their client commitments—have grown to be attractive advisors for operators and policymakers,[168] and their numbers have multiplied accordingly. And it is fair to say that the discomfort Greene identifies has been substantially reduced; intelligence community lawyers now navigate their oversight and counseling roles with little evident internal conflict.[169] The discussion above demonstrates that the basic method for bringing the two roles into alignment is that the oversight function focuses on errors and the counseling function focuses on clarity and risk. Neither asks the NSA's lawyers to assume a judge-like neutral stance: this is legal interpretation within a role of client-service and under significant bureaucratic limits. And neither the oversight function nor the counseling function asks lawyers to assess, not merely interpret and apply, the rules. Neither, that is, prompts lawyers to ask the *should* rather than the *can* question. The NSA's OGC thus exemplifies the limited, though important, impact of intelligence legalism.

Taken together, these offices instantiate NSA's strong commitment to intelligence legalism—and its strong, although perhaps lessening, disinclination to itself weighing interests and evaluating policy. Former NSA

---

[165] Greene, *supra* note 34, at 91–92.

[166] *Id*. at 92.

[167] *Id*. at 91.

[168] Even the famous contests that occurred soon after 9/11 happened on legalistic terrain: Vice President Cheney, his aide David Addington, and their DOJ lawyer-of-choice, John Yoo, dressed up their power grabs in the guise of law, complete with legal opinions. *See, e.g.*, Deputy Assistant Attorney General John Yoo, *Memorandum for the Attorney General* (Nov. 2, 2001), http://perma.cc/SK8N-4YU3. Admittedly, though, their central claim—that the executive's national security power is, as a matter of constitutional law, unfettered by purportedly constraining statute—is anti-legalistic. *See id.* ("FISA only provides a safe harbor for electronic surveillance, and cannot restrict the President's ability to engage in warrantless searches that protect the national security."; "FISA purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence. . . . Such a reading of FISA would be an unconstitutional infringement on the President's Article II authorities."). In the end, though, that claim was a gambit that failed.

[169] For analysis of the dynamics of federal lawyers' offices, *see*, for example, sources cited *supra* note 34; Thomas O. McGarity, *The Internal Structure of EPA Rulemaking*, 54 L. & CONTEMP. PROBS. 57 (1991); Elizabeth Magill & Adrian Vermeule, *Allocating Power Within Agencies*, 120 YALE L.J. 1032, 1058–62, 1072–73 (2011).

(and CIA) Director Michael Hayden put the point clearly when he said in July 2013: "Give me the box you will allow me to operate in. I'm going to play to the very edges of that box; I'm going to be very aggressive. . . . I'll get chalk-dust on my cleats, I'll be so close to the out-of-bounds markers." [170] More recently, former NSA Deputy Director Chris Inglis framed the point in terms of NSA's orientation not just towards civil liberties but more generally, describing the NSA as "an operational not a policy shop."[171]

B. Department of Justice National Security Division (NSD)

The offices just described are within the NSA. Currently, the most important external executive branch participant in NSA's compliance ecosystem is the Department of Justice, and in particular its National Security Division (NSD). NSD, headed by its own Assistant Attorney General, was established in 2006 to bring together several previously separate offices within the Department of Justice. It has grown substantially in the years since; its budget documents about 235 lawyers, divided between offices that prosecute national security crimes and offices that deal with non-prosecutorial intelligence matters. [172] The prominence of NSD in NSA matters follows from the basic legalistic approach to intelligence reform in the late 1970s and early 1980s, as embodied in FISA and Executive Order 12,333. Infusing intelligence activities with law was accomplished not only by a new substantive legal framework in FISA, subject to court enforcement, but also by empowering the Department of Justice. Indeed, it is Department of Justice lawyers who appear in the FISA court and therefore must sign off on any FISA application.[173] Thus when the NSA wanted to ask the FISA

---

[170] Interview of former NSA Director General Michael Hayden by Charlie Rose (July 29, 2013), http://perma.cc/Q83V-422B; *see also* Testimony of Michael Hayden, *Hearing before the Senate Select Committee on Intelligence*, 110th Cong., 2d Sess. (Feb. 5, 2008), at 97–98, http://perma.cc/K3J2-LLW4. ("Let me say something very clearly, Senator. I really need to put this on the record. We will play to the edges of the box that the American political process gives us. In the creation of that box, if we're asked a view, we'll give a view. But the lines drawn by that box are the product of the American political process. Once you've drawn the box, once that process creates a box, we have a duty to play to the edge of it; otherwise, we're not protecting America, and we may be protecting ourselves. . . . So there's no wink and nod here. If you create the box, we will play inside the box without exception.").

[171] Chris Inglis, Robert S. Strauss Center, *NSA at the Crossroads* (Apr. 3, 2014), https://perma.cc/QDM4-FLVR.

[172] U.S. DEP'T OF JUSTICE, FY 2013 PERFORMANCE BUDGET CONGRESSIONAL SUBMISSION Ex. I (2013), http://perma.cc/5U4A-J9RD.

[173] *See, e.g.*, U.S. DEP'T OF JUSTICE, NATIONAL SECURITY DIVISION PROGRESS REPORT 22 (2008) [hereinafter NSD 2008 PROGRESS REPORT], http://perma.cc/7WD7-YGT8 ("The Department's primary oversight in the national security realm has traditionally focused on the FBI's use of FISA and compliance with FISA Court orders—a responsibility that derived principally from our obligations as the Government's representative to the FISA Court."). Currently, this function is carried by the Operations Section of the Office of Intelligence, in NSD; prior to NSD's 2006 creation, it was performed by the Office of Intelligence Policy and Review, which sat outside any DOJ Division, and reported directly to the Deputy Attorney General. Sometimes this gatekeeping role is made explicit. *See, e.g.*,

court for permission to restart automated queries of internet metadata, it described the first step as "seeking DoJ approval."[174] Currently, this approval role is played by lawyers in the NSD Office of Intelligence. These FISA Court dynamics are similar to—although more extreme than—the ways Department of Justice lawyers influence legal matters across government in any arena subject to very frequent litigation. But even for legal questions not immediately addressed in front of the FISA Court, the views of NSD lawyers become at least close to authoritative within the executive branch, because the issue might *eventually* end up in the FISA Court. Accordingly, NSA frequently seeks legal advice not only from its own General Counsel's office but from DOJ NSD. In fact this is occasionally required by FISA minimization rules,[175] a striking departure from ordinary agency counsel practice and authority.

Moreover, since the 1980s, there have been many other equally important levers of Justice Department influence that are more unusual. The Attorney General's decisionmaking authority over the various process documents required by E.O. 12,333, discussed above, is only the most obvious example. An important separate avenue is the situations in which the Attorney General has approval authority for particular surveillance operations.[176]

In addition, there is a great deal of routine oversight work, most done by an oversight group within the NSD Office of Intelligence.[177] The NSD oversight role is institutionalized in both USSID 18 and several of the FISA minimization procedures, and comes in three flavors. First, under each of the

---

2011 Section 215 Minimization Order, *supra* note 130, § F(vii), at 13 ("Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.").

[174] Memorandum from La Forrest Williams, Deputy Assoc. Dir., Legislative Affairs Office, Nat'l Sec. Agency, to the Majority Staff Director, S. Permanent Select Comm. on Intelligence 3 (Apr. 10, 2009), http://perma.cc/Z64Z-DF47.

[175] *See, e.g.*, 2011 Section 215 Minimization Order, *supra* note 130, § F(iii), at 12 ("NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable."); Primary Order, No. PR-TT § (5)(i)(i) (FISA Ct. [date redacted]) [hereinafter Reggie Walton PR/TT Primary Order], http://www.clearinghouse.net/chDocs/public/NS-DC-0063-0002.pdf [http://perma.cc/ZA8K-HYK2] ("NSA's OGC shall consult with the Department of Justice's National Security Division (NSD) on all significant legal opinions that relate to the interpretation, scope, and/or implementation of the authorizations granted by the Court in this matter. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.").

[176] 50 U.S.C. § 1805(e); 50 U.S.C. § 1881a(a) (Section 702); USSID 18, *supra* note 49, §§ 4.1(b)(1), 4.4(b), 5.4(a) (authorizing surveillance, and retention of certain communications, on the authority of the Attorney General).

[177] National Security Division: Sections and Offices, U.S. DEP'T OF JUSTICE, http://www.justice.gov/nsd/sections-offices#oversight (last visited Nov. 7, 2014).

FISA authorities discussed in this Article, the Attorney General owes annual or semi-annual reports to Congress.[178] These reports are drafted by NSD's Office of Intelligence,[179] and necessarily require relevant agencies to report to the Attorney General the information to be passed along. Moreover, it is NSD that determines (subject, no doubt, to review and negotiation with others) how various issues are framed. The office plays a far smaller role in non-FISA collection,[180] but even then the rules sometimes similarly require reporting of particular events to the Attorney General.[181] Second, the FISA minimization rules sometimes assign DOJ lawyers a specified task. For FISA Title I surveillance, for example, NSD is required to establish procedures to "protect . . . [attorney-client] communications from review or use in any criminal prosecution, while preserving foreign intelligence contained therein."[182] And third, at least for those FISA programs we have full information on, the minimization procedures require NSD Office of Intelligence lawyers to review NSA's compliance record periodically. The review seems to range from quite minimal, for FISA Title I warrants and Section 702 foreign targeting,[183] to extremely involved, for the Section 215

---

[178] 50 U.S.C. § 1808 (electronic surveillance warrants); 50 U.S.C. § 1826 (physical searches); 50 U.S.C. § 1846 (pen/trap orders); 50 U.S.C. § 1862 (annual, business records/tangible things); 50 U.S.C. § 1871 (all of the above, plus foreign targeting orders); 50 U.S.C. § 1881a(l) (compliance assessment for Section 702 targeting and minimization); 50 U.S.C. § 1881f (Section 702, 703, 704) ("Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, concerning the implementation of this subchapter."). In addition, the Attorney General owes an annual report on FISA warrants sought, granted, modified, or denied. 50 U.S.C. § 1807.

[179] National Security Division: Sections and Offices, *supra* note 177 ("[T]he Oversight Section is responsible for meeting numerous Congressional reporting requirements, including several FISA semi-annual reports, submission of certain FISC orders to Congress, and submission of FBI statistical information.").

[180] *See, e.g.*, Testimony of John Carlin before the Senate Select Intelligence Committee (Feb. 25, 2014), at 44:37, http://perma.cc/62SW-KP6J ("But the collection activities that occur pursuant to 12333, if there was incidental collection, would be handled through a different set of oversight mechanisms than the [Justice] Department's–by the [NSA] Office of Compliance, the Inspector General there, the General Counsel there, and the Inspector General and General Counsel's office for the Intelligence Community writ large, as well as reporting to these committees as appropriate."). I was alerted to this exchange by *Does Acting National Security Division Head John Carlin Know about FISA Sections 703 and 704?*, EMPTYWHEEL (Feb. 25, 2014), https://perma.cc/WF5W-5NVU.

[181] USSID 18, *supra* note 49, § 4.1(e).

[182] USSID 18, *supra* note 49, Annex A, App. 1, § 4(a)(3)(b).

[183] For FISA Title I, NSD is required to review "at least a representative sampling" of disseminated communications, to make sure they comply with the rules on dissemination. "The results of each review shall be made available to the Attorney General or a designee." USSID 18, *supra* note 49, Annex A, App. 1, § 8(d). For FISA 702, see SECTION 702 NSA MINIMIZATION PROCEDURES, *supra* note 54, § 3(b)(6) ("The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.").

telephony metadata program.[184] NSD's role in the now-ended internet metadata program also became quite extensive, although that was not the case at the start of the program.[185] Both the second and third type of work have grown substantially since the 2004 FISA Court ratification of the internet metadata program, and particularly since 2009 compliance troubles in both the internet and telephony metadata programs and 2011 compliance troubles involving Section 702 foreign targeting. Whether at the government's behest or originating with the FISA Court judges or staff, the minimization procedures approved by the FISA Court keep adding to NSD's role.[186]

NSD lawyers have been criticized both as too interested in civil liberties and not enough in national security, and as unduly aggressive. From the right, the office has faced loud accusations that it acquiesced too readily to the view of FISA court judges that national security surveillance had to be walled off from the criminal justice system;[187] only after 9/11, and the enactment of the USA PATRIOT Act, did the Department finally appeal the issue to the FISA Court of Review, and win.[188] As former NSD lawyer Carrie Cordero summarized the history in congressional testimony, itemizing several other incidents, "the Department of Justice was accused of being too reticent, too cautious, too unwilling to be aggressive under the law in order to protect the national security."[189] From the left, however—and particularly more recently—the argument is reversed. Again quoting Cordero (who describes the shift as "ironic"), it is "that we need more lawyers scrutinizing already well-scrubbed applications; and that the government should be putting forth more cautious interpretations of the

---

[184] For the telephony metadata program, see 2011 Section 215 Minimization Order, *supra* note 130. NSD reviews all the training and briefing, and the justifications for RAS approvals for selection terms used to query the BR metadata. *Id.* at §§ F(i), (iv). In addition, NSD is assigned to meet with the NSA compliance office and General Counsel, to "assess[] compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired." *Id.* at § F(iv). Finally, NSD must meet with NSA's Office of the IG, "to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders." *Id.* at § F(v).

[185] *See* Application for Use of Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes, [Case name and docket redacted] (FISA Ct. 2004), http://www.clearinghouse.net/chDocs/public/NS-DC-0028-0002.pdf [http://perma.cc/U5SX-9UL8].

[186] *See supra* note 94.

[187] STEWART BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 31–39 (2010).

[188] In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

[189] *Continued Oversight of the Foreign Intelligence Surveillance Act: Statement for the Record Before the Comm. On the Judiciary* (Oct. 2, 2013) (footnotes omitted), http://perma.cc/HTF7-9UA4 (statement of Carrie Cordero). Cordero is the former Counsel to the Assistant Attorney General for National Security. Benjamin Wittes summarizes the same shift in LAW AND THE LONG WAR: THE FUTURE OF JUSTICE IN THE AGE OF TERROR 221 (2008).

law."[190] Cordero herself has written that neither argument is correct. Rather, she says, NSD is "a neutral party that evaluates the Intelligence Community's requests for surveillance."[191]

Admittedly, Cordero's "neutral" comment was made in a blog, and may have been a little casual. But the description above demonstrates that, structurally, NSD's lawyers are indeed expected to function, simultaneously, as lawyers for their client agencies and fair quasi-adjudicators. As Nancy Libin, the former Privacy and Civil Liberties Officer for the Department of Justice, puts it, the NSD is "this place that the IC goes to get blessed." Libin comments that this creates "a structural problem," because lawyers representing the IC "can get captured by the IC."[192] Libin's substantive point seems to me to be absolutely correct—although the term "capture" is not quite apropos, because NSD lawyers in the Office of Intelligence are not IC outsiders, but IC lawyers. Their immediate colleagues and their bosses are responsible for national security prosecutions using the fruits of the surveillance they ratify. Neither their roles, reference groups, nor career aspirations support a norm of quasi-judicial neutrality.

Stepping back a bit to evaluate all of this, NSD lawyers bring to their FISA and oversight work several key characteristics. One is the lawyerly mindset, which merges careful textual analysis and a keen eye for helpful ambiguity. Another is a commitment to their client's operational success. A third is a natural desire, as repeat players in front of the FISA court, to safeguard their own credibility. And perhaps a fourth is the embracing of rule of law values—the ideas of intelligence legalism, that law should matter in the realm of intelligence. All four characteristics are reinforced by NSD lawyers' role, reference group, and career aspirations. All four inform their approach to being *both* counsel to the government and officers of the FISA court, exhibiting candor and care but pressing aggressive pro-government positions unless those positions are rejected by the court or are likely to be rejected. Recent accounts suggest that within the Department of Justice, NSD at least occasionally takes aggressive pro-surveillance positions. Just to cite one example, until the Solicitor General directed a more defendant-friendly reading, "the division . . . long used a narrow understanding of what 'derived from' means in terms of when it must disclose specifics to defendants" explaining that evidence in their criminal case had its origin in warrantless wiretaps.[193] The point is not that NSD's lawyers were right or wrong about this position. It is that if a credible argument can be made in support of their clients' proposals, and the FISA judges have not rejected that argument, one would expect NSD lawyers to make it.

---

[190] Cordero, *supra* note 189.

[191] Carrie Cordero, *Thoughts on the Proposals to Make FISA More Friendly*, LAWFARE (Aug. 12, 2013, 1:17 PM), http://perma.cc/M67J-ASXP.

[192] Libin Interview, *supra* note 15.

[193] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 17, 2013), http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?pagewanted=2&_r=0.

And just as it is wrong to expect neutrality from NSD, it would be foolish to expect a more thorough-going civil liberties orientation. NSD's lawyers are not civil rights or civil liberties lawyers: they are not hired for their civil liberties experience or orientation towards civil liberties; they are not asked to perform a civil liberties function; and their next jobs are rarely, if ever, civil liberties jobs. It is unsurprising that when the FISA judges were building the now-dismantled "wall," those Department of Justice intelligence lawyers who frequently appeared before them would respect and even support that approach. But unlike with civil liberties lawyers, there is every reason to predict that NSD lawyers would avoid pro-civil liberties positions in the face of court indifference to the individual interests at stake—and no evidence to the contrary has thus far been disclosed.

It is worth emphasizing that NSD's lead role within the Department of Justice is less than a decade old. NSD's immediate predecessor was the Office of Intelligence Policy and Review (OIPR), a freestanding office that handled FISA and other intelligence matters.[194] OIPR was itself a 1979 offshoot of the Office of Legal Counsel (OLC); prior to its establishment, OLC lawyer Mary Lawton was the lead Department of Justice intelligence lawyer, and she maintained that role when she led OIPR for a decade.[195] During that period, contemporaries described the new office as a "'mini Office of Legal Counsel' with respect to any issue concerning intelligence policy."[196] The actual Office of Legal Counsel continued to play a crucial role as well—this is evident in the hospital bed episode described in the Introduction, which were prompted by OLC head Jack Goldsmith's qualms about the President's surveillance program,[197] and in the first telephony metadata application to the FISA Court, whose approval subjected that program to judicial supervision, which was, remarkably, signed not only by the head of OIPR but also by the head of OLC (which rarely takes formal part in litigation).[198] As with NSD lawyers, I think it would be implausible to expect neutrality from OLC lawyers; their role within the government is, in part, to defend executive prerogative.[199] At the same time, if it were OLC lawyers doing FISA oversight, the dynamics might well be quite different

---

[194] NSD 2008 PROGRESS REPORT, *supra* note 173.

[195] *Chapter Twenty: "Primary Purpose" and the Sharing of Intelligence Information Among the FBI, OIPR, and the Criminal Division*, http://perma.cc/AM4Y-6X3L.

[196] *Id*.

[197] *See* sources cited *supra* notes 1-2.

[198] *See Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism*, Docket redacted (FISA Ct. July 2009), http://chadmin.clearinghouse.net/chDocs/public/NS-DC-0009-0004.pdf [http://perma.cc/A286-GNFW]; Lederman Interview, *supra* note 15.

[199] For a discussion of OLC and how its lawyers function, see, *e.g.*, Cornelia T. Pillard, *The Unfulfilled Promise of the Constitution in Executive Hands*, 103 MICH. L. REV. 676, 710–717 (2005); Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2336–42 (2006); Trevor W. Morrison, *Stare Decisis in the Office of Legal Counsel*, 110 COLUM. L. REV. 1448, 1460–70 (2010).

than I have described. Just to name two key differences, OLC lawyers would not have the repeat appearances before the FISA Court, and they are often called upon to play a quasi-judicial role within the executive branch (their legal memoranda are even given the title of "decisions"). But while OLC lawyers continue to be extremely involved in legal issues related to national security that reach the National Security Council,[200] with the establishment and growth of NSD, led by a Senate-confirmed Assistant Attorney General, OLC's relative role with respect to FISA and surveillance has shrunk. NSD is the key FISA office within the Department of Justice.

C. Other Intelligence Oversight Offices

Other offices oversee some of the tasks and activities already described. For non-FISA matters, the Office of the Director of National Intelligence (ODNI) receives mandatory reports by each element of the Intelligence Community of "any intelligence activities of their organizations that they have reason to believe may be unlawful or contrary to executive order or presidential directive."[201] The reports are shared within ODNI with the Office of General Counsel, the Civil Liberties Protection Office, and Mission Integration Division. They are then relayed to the Intelligence Oversight Board (IOB), in the White House, along with an ODNI "assessment of the gravity, frequency, trends, and patterns of occurrences" of reportable incidents, a summary of corrective actions taken and related recommendations, and an assessment of their effectiveness.[202] This process simultaneously increases ODNI information about compliance issues across the IC, and the salience of compliance incidents within the IC elements themselves when the heads of the IC elements (and therefore many other lead officials within each element) read the relevant reports.[203] The IOB itself, currently a committee of the President's Intelligence Advisory Board, brings together non-governmental experts (usually former high-ranking government officials) to advise the President[204]; it is extremely low

---

[200] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 311 (2007).

[201] Exec. Order No. 12,333, 3 C.F.R. (1981) § 1.7(d); *see also* Exec. Order No. 12,334, 3 C.F.R. (1981); Exec. Order No. 13,462, 73 FR11805 (2008) §§ 7-8 at 11806-11807 ("[T]he DNI shall . . . receive reports submitted to the IOB pursuant to section 1.7(d) of Executive Order 12333, or a corresponding provision of any successor order"; "the heads of departments concerned shall . . . ensure that the DNI receives . . . copies of reports submitted to the IOB pursuant to section 1.7(d) of Executive Order 12333, or a corresponding provision of any successor order.").

[202] Exec. Order No. 13,462 §§ 6, 7, 8; Complaint at 3–4, Elec. Frontier Found. v. Cent. Intelligence Agency, No. C 09-3351 SBA, 2013 WL 5443048 (N.D. Cal. Sept. 30, 2013) (filed July 22, 2009), https://www.eff.org/document/complaint-16.

[203] Joel Interview, *supra* note 15.

[204] The PIAB has a small professional staff within the Executive Office of the President. *See About the PIAB*, THE WHITE HOUSE, http://perma.cc/S3Y3-LLM8 (last visited Nov. 10, 2014). The current members of the IOB are also members of the PIAB. *President's Intelligence Advisory Board and Intelligence Oversight Board: Members*, THE WHITE HOUSE, http://perma.cc/L9UL-JL2G (last visited Nov. 10, 2014). They may be less active,

profile,[205] and there is no public information on what it does with the compliance reports it receives, although FOIA requests have led to the disclosure of thousands of pages of those reports.[206]

In addition, under the DOD rules implementing Executive Order 12,333, the Assistant to the Secretary of Defense for Intelligence Oversight (abbreviated, unfortunately, ATSD(IO))[207] also receives from NSA's General Counsel and Inspector General a "quarterly report describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive order or Presidential directive, or applicable DoD policy; and actions taken with respect to such activities," as well as "significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system."[208]

Neither ATSD(IO) nor ODNI has a principal part in FISA oversight—DOJ oversight really has pride of place under FISA.[209] The

currently, than in prior years. *See* Josh Gerstein, *Obama Upends Intel Panel*, POLITICO (Aug. 15, 2013), http://perma.cc/4RQC-7UWS.

[205] In 2011, the Electronic Frontier Foundation (EFF) had to bring a FOIA litigation to find out even who the members of the IOB were. *See* Mark Rumold, *The Intelligence Oversight Board Has Members—But We Had to Sue the Government to Find Out*, ELEC. FRONTIER FOUND. (EFF) (Nov. 9, 2011), https://www.eff.org/deeplinks/2011/11/intelligence-oversight-board-has-members-and-all-we-had-do-was-sue-federal; Complaint, Elec. Frontier Found. v. Office of the Dir. of Nat'l Intelligence, No. 4:11-cv-04790-LB, N.D. Cal. (Sept. 27, 2011). Its role may have been more robust prior to its 2008 demotion by President Bush. President's Intelligence Advisory Board and Intelligence Oversight Board, Exec. Order No. 13,462, 73 FR 11805 (March 4, 2008); Charlie Savage, *President Weakens Espionage Oversight*, BOSTON GLOBE (March 14, 2008), http://www.boston.com/news/nation/washington/articles/2008/03/14/president_weakens_espionage_oversight/?page=full. Some but not all of the authority stripped from the IOB in 2008 was restored by President Obama in 2009. *See* Exec. Order No. 13,516, Amending Executive Order 13462 (October 28, 2009), 74 FR 56521 (Nov. 2, 2009), 74 FR 57241 (Nov. 5, 2009).

[206] *Intelligence Oversight Board: FOIA Documents Detailing Legal Violations*, ELECTRONIC PRIVACY INFO. CENTER, http://perma.cc/Q4MR-7WZ8 (last visited Feb. 4, 2014). See also *Transparency Project: Intelligence Agencies' Misconduct Reports*, ELEC. FRONTIER FOUND., https://www.eff.org/foia/intelligence-agencies-misconduct-reports (last visited Feb. 4, 2014) for the reports so far disclosed as a result of Elec. Frontier Found. v. Cent. Intelligence Agency, 4:09-cv-03351-SBA (N.D. Cal. filed July 22, 2009), 2013 WL 5443048 (N.D. Cal. Sept. 30, 2013).

[207] *See* Organizational Charter, Assistant to the Secretary of Defense (Intelligence Oversight), 32 C.F.R. § 378 (1983) (establishing the office of the Assistant to the Secretary of Defense for Intelligence Oversight); DEP'T OF DEF., ASSISTANT TO THE SECRETARY OF DEFENSE FOR INTELLIGENCE OVERSIGHT (DoD 5148.11, Apr. 24, 2013), http://perma.cc/Z9QY-CX5X; DEP'T OF DEF., ASSISTANT TO THE SECRETARY OF DEFENSE FOR INTELLIGENCE OVERSIGHT (DoD 5148.11, May 21, 2004), http://perma.cc/UA6D-LUCZ; DOD DIRECTIVE 5240.1-R, *supra* note 76.

[208] DOD DIRECTIVE 5240.1-R, supra note 76, at C15.3.3.2.

[209] *See* Intelligence Reform and Terrorism Prevention Act (IRTPA), Pub. L. 108-458, § 102A(f)(8), 118 Stat. 3638, 3650 (2004) (codified as amended at 50 U.S.C. § 3024(f)(9))

exception is under Section 702, where in the 2008 FISA Amendments Act, Congress expressly assigned ODNI as well as the Department of Justice to "assess compliance with the targeting and minimization procedures.[210] To produce semi-annual compliance assessments, ODNI's Office of General Counsel, Mission Integration Division, and Civil Liberties and Privacy Office all make regular appearances in the NSA compliance ecosystem, dealing with Section 702 foreign targeting and minimization. The work is done every 60 days by a small team from ODNI (joined by a larger team from DOJ NSD).[211]

Given the topic of this paper, I am most interested in the ODNI Civil Liberties Protection Office because its statutory authorities extend past legal compliance to policy development—it is authorized to look at the "should" question. One of the Office's two foundational statutes requires its leader to:

> (1) assist the head of such department, agency, or element and other officials of such department, agency, or element in appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;

and

> (4) in providing advice on proposals to retain or enhance a particular governmental power the officer shall consider whether such department, agency, or element has established—
> (A) that the need for the power is balanced with the need to protect privacy and civil liberties;
> (B) that there is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties; and
> (C) that there are adequate guidelines and oversight to properly confine its use.[212]

The reference to "civil liberties *concerns*" (emphasis added) and "balanc[ing]" suggest that this is not simply a compliance mission. ODNI's

---

("Nothing in this subchapter shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.").

[210] *See* 50 U.S.C. § 1881a(l)(1).

[211] *See* compliance reports listed *supra* note 109. *See also, e.g.*, SECTION 702 NSA MINIMIZATION PROCEDURES, *supra* note 54, § 3(b)(6). The civil liberties office's quarterly reports also tally FISA compliance reviews each quarter beginning in Sept.–Nov. 2010. *Civil Liberties Privacy Office Reports*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, http://perma.cc/KR9X-MJXZ (last visited Feb. 4, 2014).

[212] 42 U.S.C. § 2000ee-1.

Civil Liberties and Privacy Office could, with statutory warrant, play a policy role. It could push against the information imperatives, the desire to "collect it all," that motivate some at NSA,[213] urging more weight be given to individual's liberty and privacy interests as well as rights.

But if there is textual support for the idea that ODNI's Civil Liberties and Privacy Office has been assigned a civil liberties or privacy role that runs deeper than compliance, that assignment is equivocal. Other language in the office's founding statutes is geared more towards compliance with law. For example, the office is assigned by the Intelligence Reform and Terrorism Prevention Act (IRTPA) to "oversee *compliance* by the Office and the Director of National Intelligence with requirements under the Constitution and all laws, regulations, Executive orders, and implementing guidelines relating to civil liberties and privacy."[214]

Faced with this textual range, those who manage this small office have chosen to frame its role, at least publically, primarily in compliance terms. Its "enterprise strategy," for example, states: "We are committed to protecting fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law."[215] Other documents, too, omit "balancing" type language or references to "concerns," preferring harder references to "violations" and "law."[216]

Alex Joel, the office's director since its start up, explains that his approach is consciously tied to legal requirements:

> It's been attractive to me to run the office as a law shop, because we [government personnel] of course have to follow the law. We have traditionally defined privacy and civil liberties *rights* with reference to the law (including executive orders). It's important to emphasize that this is not optional, that this is what the law requires.[217]

It is not that Joel takes no position at ODNI and in interagency discussions on policy matters; in fact he states that "I try to say, just like the President recently said, 'Just because we *can* do something, doesn't mean we

---

[213] *See, e.g.*, Ellen Nakashima & Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All,'* WASH. POST (July 14, 2013). http://perma.cc/KDT3-ENU5.

[214] 50 U.S.C. § 3029(2)(b)(2) (emphasis added).

[215] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, COMMUNITY ENTERPRISE STRATEGY 2012-2017, http://perma.cc/L3ST-THAX (last visited Nov. 2, 2014).

[216] *See, e.g.*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INTELLIGENCE COMMUNITY DIRECTIVE 107: CIVIL LIBERTIES AND PRIVACY (Aug. 31, 2012), http://perma.cc/PN4Z-TLF7.

[217] Joel Interview, *supra* note 15.

necessarily should.'"[218] But Joel sees persuading colleagues about what ought to happen as harder than telling them what is required to happen,[219] and while no doubt he and others on his staff give advice on the "should" question, it is evident that with respect to the NSA, the office's focus is primarily compliance. For example, one of the Section 702 semiannual compliance reviews has been released in a form that allows evaluation of its content. Finalized in August 2013, it does not read very differently from the NSA's own released or leaked compliance work. Both deal with the precise requirements of the targeting and minimization rules and the situations in which errors have occurred. In fact, Joel has sought out detailees from DOJ NSD to serve as his office's designated staff for Section 702 compliance.[220] Moreover, the office's public statements have all been defenses of IC policies and practices.[221]

In short, the staff from these DOD, ODNI, and White House overseeing offices all conceptualize their role as ensuring that the NSA's activities comply with the rules system that exists. At least as far as one can observe from the written record so far released, none take their role to be assessing whether the rules are appropriate, or whether conduct that is compliant with the rules might nonetheless be ill advised.

D. FISA Court

In general, federal courts perform important, but limited, oversight of federal official conduct. Doctrines like ripeness, finality, and standing, and, especially, limits on inferred private rights of action, mean that courts are closed to many, even most, potential claims of agency illegality. In keeping with this ordinary situation, the vast majority of the NSA's operations lie outside court supervision. Executive Order 12,333 implements executive rather than federal court involvement, and without a statutory framework, court oversight is difficult to justify. Would-be challengers not only lack knowledge that they are subject to surveillance and therefore have standing to bring a challenge[222]; as foreigners abroad, under current doctrine, they often lack constitutional rights altogether.[223] (Although Presidential Policy

---

[218] *Id.* (quoting President Barack Obama, Press Conference (Dec. 20, 2013), http://perma.cc/399F-2U2Z).

[219] Joel Interview, *supra* note 15.

[220] *Id*.

[221] Civil Liberties and Privacy Office, ODNI, *Civil Liberties and Privacy Information Paper: Description of Civil Liberties and Privacy Protections Incorporated in the 2008 Revision of Executive Order 12333* (orig. Aug. 2008; edited Aug. 2013), http://perma.cc/XRC7-WBQB; Alexander W. Joel, *The Truth About Executive Order 12333*, POLITICO (Aug. 18, 2013), http://perma.cc/7WQT-FGLG.

[222] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

[223] United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990).

Directive 28, announced by the President in January 2014, requires consideration of the privacy interests of foreigners abroad.[224])

In the portion of its operations that proceed under FISA, however, in many ways, the NSA lives with much more court oversight than do most federal agencies. Most federal agencies, after all, do not need before-the-fact court approval for routine operations. And while FISA warrants are similar to criminal justice warrants, which issue with court approval, FISA metadata programs actually involve much more court supervision than do the FBI's National Security Letters.[225] The result has been intense judicial involvement in enforcement of the minimization rules—court orders, once approved. In opinion after opinion, in both the internet and telephony metadata programs and Section 702 targeted surveillance of foreigners abroad, FISA court judges have delved into compliance incidents, their sources, and their remedies.[226] At the same time, FISA judges have devoted many fewer pages of the opinions so far declassified to the legitimacy—both statutory and constitutional—of those NSA programs. Most starkly, it took over seven *years* before any FISA judge actually wrote an opinion explaining the Court's repeated decisions to uphold bulk telephony metadata collection programs.[227]

The opinions suggest that the court is supervising the surveillance process with close attention—but not adjudicating its merit. And in some ways, that approach is inherent in the judicial role. I have distinguished throughout this Article between "rights" or "compliance" or "law" on the one hand, and "interests" or "balancing" or "policy" on the other. Courts, including the FISA Court, sit on the law side of that divide. The dynamics of judicial law-pronouncement are, however, very different than for executive compliance work. Executive branch lawyers' role commits them to the search for "'yes' when it can be," even if they are simultaneously capable of delivering "'no' when it must be." And executive lawyers tend to consider their clients' preferences close to binding on policy issues, when such issues

---

[224] *See* EXEC. OFF. OF THE PRES., PRESIDENTIAL POLICY DIRECTIVE 28 – SIGNALS INTELLIGENCE ACTIVITIES (Jan. 17, 2014) [hereinafter PPD-28], http://perma.cc/3AQQ-PKE2 ("These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside."); *id.* § 4 ("All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.").

[225] For information on National Security Letters, *see, e.g.*, 1 KRIS & WILSON, *supra* note 32, ch. 19.

[226] *See supra* notes 91–94 and accompanying text.

[227] In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things From [Redacted], No. BR 13-109 (FISA Ct. Oct. 11, 2013), http://www.clearinghouse.net/chDocs/public/NS-DC-0017-0001.pdf [http://perma.cc/3YYT-XXWR].

arise. Judges, by contrast, begin with a norm of impartiality rather than client service, and are far less constrained with respect to whatever policy issues bear on their legal decision-making, as well as with respect to legal interpretation itself. Thus the FISA Court *could* serve as a body that engages in the "should" question, at least to some extent, as part of the legal interpretive process. Other courts examining the permissibility of the NSA's FISA surveillance have done just that.[228]

That the FISA Court did not take on the "should" question in any significant way, prior to the Snowden disclosures, may be in part due to the absence of adversarial briefing, as elaborated upon in Part IV.[229] But my sense is that one-sided briefing is only part of the explanation. The FISA Court's one-party procedures have a deeper impact, as well. The ex parte modality alters not just *who* communicates with the court but *how* the government and court communicate with each other. Sometimes FISA judges make their influence felt by the traditional judicial process of issuing a decision: the 2009 order suspending the NSA's access to internet metadata[230] is one example. But much more often, facilitated by the ex parte nature of the proceedings, it seems that the court's views are delivered in the form of less formal advice to the government. ODNI General Counsel Robert Litt explained in congressional testimony in 2013:

> When we prepare an application for a FISA [order], whether it's under [Section 702] or a traditional FISA [warrant], we first submit to the court what's called a read copy, which the court staff will review and comment on. And they will almost invariably come back with questions, concerns, problems that they see, and there's an iterative process back and forth between the government and the FISA court to take care of those concerns so that at the end of the day we're confident that we're presenting something that the FISA Court will approve. That is hardly a rubber stamp. It's rather extensive and serious judicial oversight of this process.[231]

---

[228] *See e.g.*, Klayman, 957 F. Supp. 2d. 1.

[229] As District Judge William Pauley noted in Am. Civil Liberties Union v. Clapper, "The two declassified FISC decisions authorizing bulk metadata collection do not discuss several of the ACLU's arguments. They were issued on the basis of *ex parte* applications by the Government without the benefit of the excellent briefing submitted to this Court by the Government, the ACLU, and *amici curiae*. There is no question that judges operate best in an adversarial system." Clapper, 959 F.Supp. 2d at 756.

[230] In re Prod. of Tangible Things from [Redacted], No. BR 08-13 (FISA Ct. Mar. 2, 2009), 2009 WL 9150913, http://www.clearinghouse.net/chDocs/public/NS-DC-0011-0005.pdf [http://perma.cc/X938-9KMH] ("[E]xcept as authorized below, the Court will not permit the government to access the data collected until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data.").

[231] *How Disclosed NSA Programs Protect Americans, and why Disclosure Aids Our Adversaries*: *Hearing before the H. Permanent Select Comm. on Intelligence*, 113th Cong. (June 18, 2013) (testimony of Robert Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence), http://perma.cc/77WZ-W9H5 (last visited Nov. 30, 2014).

One-party process thus accommodates a back-and-forth in which the government gets several tries to alter—or, although Litt didn't say so, withdraw—its applications to avoid being turned down.[232] Often, as Litt describes, the government is dealing not with a judge but with the FISA Court's handful of "legal advisors."[233] These are long-term lawyer assistants to the judges, who likely possess more influence than ordinary law clerks, because they are experienced attorneys with government backgrounds in surveillance law who serve for years at a time. They may therefore have more expertise than the judges themselves, particularly towards the start of the judges' seven-year terms.[234]

Even when the contact between the government and the court involves the judges directly, it is clear that the procedures are sometimes closer to a congressional briefing, say, than an ordinary judicial hearing, even an ex parte one. For example, the NSA provided Senate Intelligence Committee with the following description:

> On September 1, 2009, at the request of the FISC, NSA hosted Presiding Judge Bates and Judges Walton and Hogan for a series of briefings and demonstrations regarding the BR FISA program. The presenting included a briefing on BR FISA data flow; a demonstration of how analysts log on to NSA systems to access BR FISA data; a demonstration of technical safeguards that prevent queries based on seed numbers that do not mean the Reasonable Articulable Suspicion (RAS) standard; and a demonstration of analyst queries using RAS-approved telephone identifiers. The information was presented in the context of a current operation that concerns a potential threat to the U.S. homeland. . . . The judges were engaged throughout and asked questions, which were answered by the briefers and other subject matter experts. At the conclusion, the judges expressed their appreciation for the amount and quality of information presented to them.[235]

The briefing included a "working lunch," and, as with so many such sessions, a PowerPoint slide deck, complete with bullet points on the

---

[232] It seems as well that the FISA Court also modifies the orders. *See, e.g.*, Letter from Peter J. Kadzik, Principal Deputy Assistant Att'y Gen., to Sen. Harry Reid, Majority Leader (Apr. 30, 2013), http://perma.cc/39U6-6LA2 (reporting that the FISA Court modified 200 of the 212 applications for Section 215 orders).

[233] *Id.*

[234] On the legal advisors, see 1 KRIS & WILSON, *supra* note 32, § 5.3.

[235] Memorandum from Ethan L. Bauman, Assoc. Dir., Legislative Affairs Office, Nat'l Sec. Agency to the Staff Director, Senate Select Committee on Intelligence (Sept. 10, 2009), https://perma.cc/8YEG-S6M8.

session's purpose ("Demonstrate NSA's dedication to compliance with the Court Orders and demonstrate how NSA uses the BR FISA program operationally in its counterterrorism missions while appropriately protecting U.S. person privacy").[236] It was apparently effective: on September 3, 2009, the Court allowed the NSA to resume analysis of the Section 215 telephony metadata suspended six months earlier.[237]

Of course trial court judges in other courts deal with litigants in a variety of contexts and using many approaches.[238] But the episodes just described—advice-giving, iterative drafting, briefings—depart significantly from the ordinary judicial mode, even while the FISA Court evidently maintains enormous influence over FISA surveillance. It seems almost unavoidable that this type of collaboration leads to a sense of shared effort and enterprise. Other practices, such as an annual lunch bringing together FISA Court judges and legal advisors (and the Chief Justice) with the heads of the CIA, NSA, and FBI[239] likewise encourage the judges to conceptualize themselves as participating with the IC in a common project. In any event, while the FISA court superintends the surveillance process, clearly it does not evaluate whether it should go forward at all. That superintendence is rigorous, but limited.

E. PCLOB

Of the oversight institutions thus far described, only NSA's brand-new Civil Liberties and Privacy Office engages in policy-type weighing of civil liberties interests against the security benefits offered by particular surveillance methods. The one office that remains to be discussed is the Privacy and Civil Liberties Oversight Board (PCLOB), an independent bipartisan agency nominally within the executive branch.[240] As will be seen, and as one would expect from what is essentially a blue-ribbon-commission type organization with no enforcement or other executive function, the PCLOB seems so far to be functioning at least partially free of the role constraints of an executive agency.

In its first incarnation, as part of the Executive Office of the President,[241] the PCLOB was an unimportant player in NSA's operations. In

---

[236] Business Records FISA: Presentation for the Foreign Intelligence Surveillance Court (Sept. 1, 2009), http://perma.cc/B567-W4CY.

[237] In re Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things From [redacted], No. BR 09-13, 2009 WL 9150914 (FISA Ct. Sept. 3, 2009), http://www.clearinghouse.net/chDocs/public/NS-DC-0015-0001.pdf [http://perma.cc/S9MZ-E43N]; Bauman Memorandum, *supra* note 235.

[238] *See, e.g.*, JUDITH RESNIK, *Managerial Judges*, 96 HARV. L. REV. 374 (1982).

[239] Conversation with former FISA Court judge (October 8, 2014).

[240] *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (codified at 42 U.S.C. § 2000ee (2012)).

[241] *See* Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108–458, title I, § 1061, 118 Stat. 3684 (2004).

its second, independent, incarnation,[242] it started operations only recently. President Obama was slow to name the Board's members, and the Senate was even slower to confirm them[243] Its budget is tiny; it has only a handful of full-time staff members (one on a detail from the Department of Justice), in addition to its full-time chair and part-time members.[244] But after David Medine's long-awaited confirmation as chair in May 2013,[245] the Snowden disclosures, one week later, prompted the Board to undertake a review of FISA, the first part of which it completed in January 2014.[246]

The board's statute commits it firmly to a policy, *not* compliance, function, requiring it to:

> (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
>
> (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.[247]

Nonetheless, in its review of the telephony metadata program, the board began with the language of law. Three of its five members—the three Democrats—found that Section 215 "does not provide an adequate legal basis to support the program," and that the program also violates the Electronic Communications Privacy Act.[248] The Board acknowledged that the FISA Court had approved the program many times, but explained that it found that approval unpersuasive: "Having independently examined this statutory question, the Board disagrees with the conclusions of the government and the FISA court."[249] Pointing out that the program long predated its authorization by the FISA Court under Section 215, the Board concluded, after forty-five pages of statutory analysis: "It may have been a laudable goal for the executive branch to bring this program under the

---

[242] *See* Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee, Pub. L. 110–53, title VIII, § 801(a), 121 Stat. 352 (2007).

[243] Scott Shane, *The Troubled Life of the Privacy and Civil Liberties Oversight Board*, N.Y. TIMES (Aug. 9, 2012), http://perma.cc/7XKE-NTSQ.

[244] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: STAFF BIOGRAPHIES, http://www.pclob.gov/about-us/staff.html (last visited Oct. 20, 2014).

[245] David Firestone, *A Chance for Oversight on Civil Liberties*, N.Y. TIMES (July 3, 2013), http://perma.cc/B6CZ-NAFB.

[246] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORD PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, Annex B, 214 (Jan. 23, 2014) [hereinafter PCLOB, 215 REPORT], http://perma.cc/FA8U-6RFJ.

[247] 42 U.S.C. § 2000ee(c) (2012).

[248] PCLOB, 215 REPORT, *supra* note 246, at 10.

[249] *Id.* at 57.

supervision of the FISA court. Ultimately, however, that effort represents an unsustainable attempt to shoehorn a preexisting surveillance program into the text of a statute with which it is not compatible."[250] Accordingly, it wrote, the program should be halted.[251]

The Board also analyzed the constitutional law issues raised by the telephony metadata program. It explained that under the Supreme Court's existing doctrine, a Fourth Amendment challenge would fail. "It is possible that the third-party doctrine or its scope will be judicially revised," the Board wrote—making clear its own view that this revision would be very welcome. "To date, however, the Supreme Court has not modified the third-party doctrine or overruled its conclusion that the Fourth Amendment does not protect telephone dialing records. Most courts continue to follow those precedents, and government lawyers are entitled to rely on them, including in their formulation and defense of the Section 215 program."[252] On First Amendment associational rights, the Board noted that standing doctrine had so far obstructed full court testing of the rights, but that the challenge was far from trivial.[253]

It should be evident, then, that the PCLOB's perspective on "the law" was quite different from that of any federal agency staff. In its first report, its members, among them a retired federal court of appeals judge, assumed much more the stance of court of appeals judges. Holdings by courts that are not the Supreme Court were treated as potentially persuasive, but not binding. And even Supreme Court holdings were deemed potentially undermined by subsequent changes of circumstances or surrounding doctrine. The PCLOB members obviously felt far freer than agency counsel do with respect to legal analysis and interpretation; the analysis is not only of precedent but also, in more typically judicial mode, of the policy pros and cons. The result was that the board took advantage of the authority of the law/compliance frame, without many of the constraints that frame usually imposes on executive branch officials. Its pronouncement that the telephony metadata program is illegal, beyond the statutory authority of the administration, is what got by far the most attention.[254]

The PCLOB's two Republican appointees disagreed with the three Democrats both on the merits and on the Board's role. One wrote:

> This *legal* question will be resolved by the courts, not by this Board, which does not have the benefit of traditional adversarial legal briefing and is not particularly well-suited

[250] *Id.* at 102.
[251] *Id.*
[252] *Id*. at 104.
[253] *Id*. at 105–06.
[254] *See*, *e.g.*, Charlie Savage, *Watchdog Report Says N.S.A. Program Is Illegal and Should End*, N.Y. TIMES (Jan. 23, 2014), http://perma.cc/3C8L-3CYV.

> to conducting de novo review of long-standing statutory interpretations. We are much better equipped to assess whether this program is sound as a *policy* matter and whether changes could be made to better protect Americans' privacy and civil liberties while also protecting national security.[255]

To be clear, the Democratic PCLOB members also addressed the policy considerations on their own merits, and urged that those considerations be implemented as new law. Having described the telephony metadata program as extending beyond current statutory parameters, the PCLOB emphasized that the solution was not simply shoring up FISA:

> The Board also recommends against the enactment of legislation that would merely codify the existing program or any other program that collected bulk data on such a massive scale regarding individuals with no suspected ties to terrorism or criminal activity. While new legislation could provide clear statutory authorization for a program that currently lacks a sound statutory footing, any new bulk collection program would still pose grave threats to privacy and civil liberties.[256]

The telephony metadata program was insufficiently central to the counterterrorism enterprise to justify those threats, the Board argued. "Given the significant privacy and civil liberties interests at stake, Congress should seek the least intrusive alternative and should not legislate to the outer bounds of its authority."[257] It then proceeded to make several smaller gauge recommendations about operation of the telephony metadata program, presumably in case Congress rejected the first recommendation, and continued the program in existence.

No experience facilitates evaluation of the PCLOB's effectiveness, but its 215 report is certainly adding to the current pressure for a new wave of intelligence reform. On the other hand, the independence exhibited by its first report may induce subsequent appointing Presidents to choose tamer members.

The PCLOB's second report, about targeted surveillance of foreigners abroad, under FISA § 702, similarly looked at both law and policy. But on this one, a divide among PCLOB members and inconsistent

---

[255] RACHEL BRAND, SEPARATE STATEMENT: REPORT ON THE TELEPHONE RECORD PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 3 (Jan. 23, 2014), http://perma.cc/TXY6-S825.

[256] PCLOB, 215 REPORT, *supra* note 246, at 169.

[257] *Id.* at 169.

language made the message much less clear. Much of Section 702 surveillance was appropriate, the report said. But:

> Outside of this fundamental core, certain aspects of the Section 702 program raise questions about whether its impact on U.S. persons pushes the program over the edge into constitutional unreasonableness. Such aspects include the scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, the collection of MCTs that predictably will include U.S. persons' Internet communications unrelated to the purpose of the surveillance, the use of database queries to search the information collected under the program for the communications of specific U.S. persons, and the possible use of communications acquired under the program for criminal assessments, investigations, or proceedings that have no relationship to foreign intelligence.[258]

The Board declined to decide whether the 702 program was constitutional, statutorily authorized, or not. "[R]ather than render a judgment about the constitutionality of the program as a whole, the Board instead has addressed the areas of concern it has identified by formulating recommendations for changes to those aspects of the program."[259] It elaborated:

> Because the same factors that bear on Fourth Amendment reasonableness under a 'totality of the circumstances' test are equally relevant to an assessment based purely on policy, the Board opts to present its proposals for changes to the Section 702 program as policy recommendations, without rendering a judgment about which, if any, of those proposals might be necessary from a constitutional perspective.[260]

The Board emphasized the room this approach opened to it. Constitutional avoidance, it stated:

> permits us to offer the recommendations that we believe are merited on privacy grounds without making finetuned determinations about whether any aspect of the status quo is constitutionally fatal, and without limiting our

---

[258] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 96–97 (July 2, 2014) [hereinafter PCLOB, 702 REPORT], http://perma.cc/M439-GAKN.

[259] *Id.* at 97.

[260] *Id.*

> recommendations to changes that we may deem constitutionally required.[261]

But other language the report used sounded rather more accepting. Rather than ducking the legal issues, on other pages it seemed that the Board was worried not whether the 702 program *crossed* the constitutional line, but whether it skirted a bit too close for comfort, while still remaining on the lawful side. For example:

> [C]ertain aspects of the Section 702 program push the entire program close to the line of constitutional reasonableness. . . . With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

This reading of the report as ratifying the legality (rather than declining to address the legality) of the 702 program was pushed by the Board's two Republicans, Rachel Brand and Elisebeth Collins Cook, each of them a former Bush Administration head of the Justice Department's Office of Legal Policy.[262] They emphasized in a separate statement that:

> The Board makes a few targeted recommendations to address concerns raised by . . . two aspects of the program. We stress that these are *policy*-based recommendations designed to tighten the program's operation and ameliorate the extent to which these aspects of the program could affect the privacy and civil liberties of U.S. persons. We do not view them to be essential to the program's statutory or constitutional validity.[263]

Two members, Chair David Medine and former Judge Patricia Wald, opined in a separate statement that the recommendations were needed not merely to avoid a *potential* legal problem, but to solve both constitutional and statutory infirmities already extant:

> [W]e feel strongly that the present internal agency procedures for reviewing communications and purging those portions that are of no foreign intelligence value prior to use

---

[261] *Id.*

[262] *See Biography of Rachel L. Brand--Board Member, Privacy and Civil Liberties Oversight Board*, PCLOB, http://perma.cc/F7R9-7VJA (last visited Nov. 17, 2014); *Biography of Elisebeth Collins Cook—Board Member, Privacy and Civil Liberties Oversight Board*, PCLOB, http://perma.cc/2VM4-DRZT (last visited Nov. 17, 2014).

[263] PCLOB, 702 REPORT, *supra* note 258, at 161.

> of the information are wholly inadequate to protect Americans' acknowledged constitutional rights to protection for private information or to give effect to the statutory definition of foreign intelligence information, which, as discussed below, provides a more stringent test for information relating to Americans.[264]

Evidently, however, they were unable to persuade their colleagues, and their legal conclusions were portrayed in media coverage as a dissent-type minority position. Indeed, the Board was widely perceived as having blessed the program. The *Washington Post*, for example, summarized the report as "conclud[ing] that a major National Security Agency surveillance program targeting foreigners overseas is lawful and effective but that certain elements push 'close to the line' of being unconstitutional."[265] The fairer reading of the previously-quoted language of the report—that it avoided any determination on the legal question by an incompletely theorized agreement as to recommendations—received no play in the media.

The PCLOB's ten recommendations relating to the 702 program have not received nearly as much attention as its 215 recommendations—lacking the strong legitimating language of rights and compliance, its policy ideas seem not to be gaining much traction.

III. The Liberty Gap

I observe above that American intelligence legalism has three features: substantive rules, judicial review, and empowerment of lawyers. These three together promote the compliance mindset that is evident in Part II—a mindset that at NSA is fairly longstanding, prioritized, and adequately staffed. Thus far I have offered an organizational account of a concomitant civil liberties gap: I have demonstrated that few institutional resources relating to the NSA are devoted to asking the "should" question rather than the "can" question. But perhaps this is an appropriate allocation of labor. Perhaps the "should" question *belongs* outside the NSA, indeed outside the IC—with the courts, the Congress, or the President. If these "upstream" actors could harden optimal policy into compliance-ready rules—law—then there would be no need for additional policy work within the IC. Instead, intelligence legalism might be the best implementation method.

I suggest in Section A, below, that the law alone is not enough; it is implausible that constitutional, statutory, and binding executive rules will be sufficiently robust to produce the best policy outcomes. There will always be liberty gaps—and these will increase with the passage of time from the last public outcry and resulting intervention. In Section B, I examine and reject a

---

[264] *Id.* at 153 (footnote omitted).

[265] Ellen Nakashima, *Independent Panel: NSA Surveillance Program Targeting Foreigners is Lawful*, WASH. POST (July 1, 2014), http://perma.cc/P6PA-G7NW.

different argument that intelligence legalism sufficiently furthers liberty: that lawyers, empowered by legalism, turn out to be excellent good civil liberties guardians. Finally, in Section C, I argue that the compliance focus, and the prevalence of rights and law talk, actually dampens the prospects of civil liberties policymaking, both by crowding it out and by rendering surveillance more politically acceptable and therefore making political or policy-based claims for reform less likely to succeed, whether inside the Intelligence Community or in the polity as a whole. In sum, intelligence legalism may further individual liberty to some extent, but compliance matters are apt to receive so much attention and even prestige that law functions as a ceiling rather than a floor. To add policy considerations on top of law thus requires focused intervention, discussed in Part IV.

A. The Limited, Though Important, Reach of Legality

If the Constitution and statutes (both as interpreted by judges), and binding executive orders—taken together, the law—specify optimal security/liberty policy, then intelligence legalism might be the best implementation method for that policy. But I argue this is not the case; the law is likely to be suboptimal with respect to liberty. More analytic precision may be useful here. I mean, more exactly, that law is likely to leave unregulated many situations when (a) liberty can be enhanced without a negative impact on security, or (b) when enhancing liberty *would* (or might) negatively affect security, but on balance the gain to the former is worth the hit to the latter.[266] Of course, different observers may disagree whether any particular scenario qualifies under either criterion. My point is that the limited ambitions of constitutional law and the limited political payoff from statutory or regulatory enactment of civil liberties protections mean that it is implausible on any account that the law achieves policy optimality, even for a brief moment in time. Moreover, even if that were not so, the limits in coverage of legislative-type rules—which are inevitable, and likely to grow over time—inevitably mean that there is space between the standard of "liberty where there's no, or acceptable, security cost" and the compliance-ready rules.

1. The Constitution

Consider, first, the Constitution, as interpreted by the courts. Those who answer charges of surveillance overreach by emphasizing the constitutionality of the contested conduct—which is to say, nearly every federal official who has defended the NSA in recent months—are essentially arguing that constitutional law sets not individual rights minima, but rather, perhaps even definitionally, the right civil liberties policy. If this were

[266] One way to put this is that law is unlikely to place us on the "security-liberty frontier," as defined in ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY AND THE COURTS (2007).

correct, optimal policy could be implemented by a robust compliance infrastructure. The best civil liberties path might, for example, be simply to augment judicial review, perhaps by cutting through the large variety of litigation barriers (including doctrines of ripeness, finality, standing, justiciability, state secrets, and limits on inferred private rights of action) that often impede judicial supervision.

The problem is that to assume, as this view does, that "constitutional" and "good" are the same is to mistake the role of constitutional law.[267] The distance between "constitutional" and "good" is a matter of both method and purpose. Methodologically, many of the constitutional considerations—precedent, text, framers' intent, and so on—are irrelevant to policy evaluation. Courts may well also "lack the institutional capacity to easily grasp the privacy implications of new technologies they encounter," as Orin Kerr has argued at length.[268] But even when courts include policy analysis in their decision-making, constitutional decisions at least purport to be more about "can" than about "should." That is why Fourth Amendment caselaw, notwithstanding its policy-heavy reasonableness inquiry, is formulated to give the government a good deal of leeway[269]—both for mistakes[270] and for differences of opinion.[271] Indeed, it is only to be expected that courts are likely to err on the side of non-intervention in constitutional cases. The remedial rigor that is at least the symbolic entailment of a right must on the margin discourage rights declaration [272] ; declaring something to be a "right" ups the stakes considerably, discouraging partial solutions.

---

[267] *See, e.g.*, Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 831 (2004) ("These cases suggest that courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies.").

[268] *Id.* at 858, 857–887. For more pro-court discussions of the institutional issues, *see, e.g.*, David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, (forthcoming U. Chi. L. Rev.), http://perma.cc/45VD-3L3E; Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, The Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485 (2013).

[269] *See, e.g.*, Kerr, *supra* note 267, at 838 ("[U]nderstood as a whole, the existing body of doctrine reflects a relatively humble and deferential judicial attitude.").

[270] *See, e.g.*, Brinegar v. United States, 338 U.S. 160, 176 (1949) (Fourth Amendment rules "seek to give fair leeway for enforcing the law in the community's protection. Because many situations which confront officers in the course of executing their duties are more or less ambiguous, room must be allowed for some mistakes on their part."); Graham v. Connor, 490 U.S. 386,396 (1989) ("[R]easonableness . . . must be judged from the perspective of a reasonable officer on the scene, rather than with the 20/20 vision of hindsight.").

[271] *See, e.g.*, Michigan Department of State Police v. Sitz, 496 U.S. 444, 453-54 ("the choice among . . . reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources, including a finite number of police officers").

[272] Daryl J. Levinson, *Rights Essentialism and Remedial Equilibration*, 99 COLUM. L. REV. 857, 884-885 (1999) (describing this relationship between rights and remedies as "remedial deterrence," whose "defining feature is the threat of undesirable remedial consequences motivating courts to construct the right in such a way as to avoid those consequences").

So while constitutional law and court enforcement of it sometimes advance individual liberty with respect to particular issue or in some cases, there is likely to be considerable distance between optimal policy and the constitutional floor. To quote one summary, again by Orin Kerr, "we should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies. . . . Additional privacy protections are needed to fill the gap between the protections that a reasonable person might want and what the Fourth Amendment actually provides."[273]

This position is not without its high-profile detractors. Most recently, many in the George W. Bush administration took the stance that it was generally advisable to "act to the edges of the law."[274] Accordingly, Jack Goldsmith recounts, "[a] White House confident about what it wanted to do . . . used lawyers, and especially legal opinions by OLC lawyers, as a sword to silence of discipline a recalcitrant bureaucracy."[275] But for the reasons just explained, the approach in question—call it the "chalk on the cleats" attitude—systematically fails to subject particular policies to actual merits analysis. To quote Goldsmith again, "It got policies wrong, ironically, because it was excessively legalistic, because it often substituted legal analysis for political judgment, and because it was too committed to expanding the President's constitutional powers."[276]

The Bush White House's ideas notwithstanding, the position that "constitutional" and "good" may have quite a distance between them has mostly been uncontroversial in the world of intelligence. FISA itself imposes a statutory warrant requirement—one that the Supreme Court has never held is constitutionally required. In the *Keith* case, the Supreme Court held that domestic national security surveillance required a warrant, but expressly declined to examine "the issues which may be involved with respect to activities of foreign powers or their agents."[277] The Court expressly invited legislation:

> Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.[278]

---

[273] Kerr, *supra* note 267, at 838.
[274] GOLDSMITH, THE TERROR PRESIDENCY, *supra* note 34, at 131.
[275] *Id*. at 130.
[276] *Id*. at 102.
[277] United States v. U.S. District Court, 407 U.S. 297, 322 (1972).
[278] *Id*. at 322–23.

FISA's passage was spurred in part by the *Keith* opinion's implicit threat that, absent some kind of institutionalized framework to safeguard reasonable expectations of privacy, the Court might subsequently hold that *Katz*'s warrant requirement for electronic eavesdropping covers foreign intelligence surveillance of domestic communications.[279] But it was also prompted by an emerging view in the lower courts that warrants would *not* be required.[280] As Laura Donohue summarizes in a comprehensive forthcoming article about FISA Section 702, "Congress crafted the legislation to ensure that domestic electronic foreign intelligence collection could not proceed absent prior judicial review, demonstration of probable cause, and particularity."[281] When Congress took the Court's invitation and legislated, requiring warrants for foreign intelligence surveillance at home (but leaving regulation of surveillance abroad for another day[282]), it therefore went beyond existing caselaw.

Even if one interprets FISA as implementing a constitutionally compelled framework, albeit one never articulated by a court,[283] it is clear that for many other topics in intelligence policy our current understanding of appropriate conduct is extra-constitutional. On issue after issue, for example, the Church Committee declined to rest on the Constitution (about which, it

---

[279] *See, e.g.*, 124 CONG. REC. 36, 409 (1978) (remarks of Rep. Robert Kastenmeier) ("Mr. Speaker, it has now been over 6 years since the Supreme Court in the famous Kieth [sic] case cast a cloud over current warrantless procedures for foreign intelligence surveillance. . . . Finally, after years of work by four congressional committees and two administrations, we have developed a bill. . . .").

[280] For cases upholding pre-FISA warrantless surveillance under a "foreign intelligence exception" to the Fourth Amendment's warrant requirement, see United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); United States v. Butenko, 494 F.2d 593, 602 n.32, 605 (3d Cir. 1974), *cert. denied sub nom.*; Ivanov v. United States, 419 U.S. 881 (1974); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980). Coming out the other way (albeit in dicta) was Zweibon v. Mitchell, 516 F.2d 594, 618-20 (D.C. Cir. 1975) (en banc, Skelly Wright, J.) (plurality opinion suggesting that a warrant may be required even in a foreign intelligence investigation), *cert. denied*, 425 U.S. 944 (1976). For liberals in Congress, the possibility that the Supreme Court's threat might evaporate provided additional reason to legislate.

[281] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y (forthcoming 2015).

[282] H. Rep. No. 95-1283, pt. I, at 51 (June 5, 1978) ("The fact that this bill does not bring the overseas surveillance activities of the U.S. intelligence community within its purview, however, should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans. The committee merely recognizes at this point that such overseas surveillance activities are not covered by this bill.").

[283] Donohue, for example, labels the result a "de facto Fourth Amendment standard." Donohue, *supra* note 281, at 111. The shape of any foreign intelligence exception to the warrant requirement was for decades mooted by FISA, but is being litigated again as a result of 702 surveillance (and its predecessor surveillance under the Protect American Act). *See* In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008); [Caption Redacted] 2011WL 10945618, at 24 (FISA Ct. Oct. 3, 2011); United States v. Mohamud, No. 3:10-CR-00475, 2014 WL 2866749 (D. Ore. June 24, 2014).

must have mattered, Senators' views are not dispositive). Instead, the Committee proposed a large number of new substantive rules; this included not only rules eventually incorporated in FISA[284] but also rules against assassination of foreign leaders;[285] use of academics for CIA operations without disclosure to their university presidents;[286] non-public sponsorship of books, articles, etc. by the CIA;[287] CIA relationships with journalists affiliated with U.S. media organizations, or with American clergy;[288] dangerous and unconsented human drug experimentation;[289] and so on. These recommendations constituted the Committee's views not of what was already legally required, but what *should be* required. Implementation then took place via E.O. 12,333.

2. Statutory Law

So there has long been agreement that the Constitution alone is insufficient to achieve optimal civil liberties protections with respect to surveillance. What about non-constitutional law? Are the statutes that have been passed sufficient? Or, even if they are not, might new statutory law—which can then be implemented via intelligence legalism—be the best way to fill the gap that remains after constitutional adjudication?

Start with the small subset of the Church Committee's proposed reforms implemented by FISA. The statutory text imposes a probable cause requirement for domestic surveillance for foreign intelligence purposes, as the Supreme Court hinted in the *Keith* case it might someday require as a matter of constitutional law. FISA's other contributions are procedural rather than substantive. I have suggested that optimal policy requires calibration of privacy and surveillance—that surveillance should be conducted only when its security benefits outweigh its privacy infringement. FISA includes no such constraint. Rather, to the extent surveillance requires an invasion of U.S. person privacy, FISA allows that invasion to occur, directing implementation to "minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons" only insofar as such minimization is "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[290] Thus FISA categorically gives security more weight than liberty; its text directs that any foreign intelligence "need" trumps privacy.

---

[284] II CHURCH COMMITTEE REPORT, *supra* note 20, at 308 (recommendation 13), 308–10 (recommendations 14-19).
[285] INTERIM CHURCH COMMITTEE REPORT, *supra* note 24, at 281–85.
[286] *Id.* at 456 (recommendation 42).
[287] *Id.* at 456 (recommendation 45).
[288] *Id.* at 456 (recommendation 48).
[289] II CHURCH COMMITTEE REPORT, *supra* note 20, at 308 (recommendation 12).
[290] 50 U.S.C. §§ 1801(h)(1). *Compare* § 1821(4)(A), *with* § 1861(g)(2)(A).

You may be thinking that the Congress that enacted FISA chose a thumb on the scale for security because it disagreed with me on the merits, believing that FISA's trump card for security constituted optimal policy. That is, perhaps the 1978 Congress saw FISA as closing whatever civil liberties gap there was. The historical record suggests otherwise, however. Reformers in the 1970s made clear that they didn't intend for congressional protection of civil liberties against surveillance to end with FISA. Rather, the Church Committee's view was on top of FISA itself, executive/congressional disclosure would both minimize the future use of liberty-infringing techniques and facilitate future interventions The Committee made formal findings that Congressional dereliction of oversight responsibilities had "helped shape the environment in which improper intelligence activities were possible."[291] Accordingly, it explained:

> Procedural safeguards—"auxiliary precautions" as they were characterized in the Federalist Papers—must be adopted along with substantive restraints. . . . Our proposed procedural checks range from judicial review of intelligence activity before or after the fact to formal and high level Executive branch approval and more effective Congressional oversight.[292]

Committee members (Senators) evidently believed that the congressional disclosure it urged would facilitate liberty as well as accountability, allowing future lawmakers to intervene where salutary, using either soft or hard methods, to appropriately balance liberty and security. As Loch Johnson—first Senator Church's special assistant, then the first staff director of the House Subcommittee on Intelligence Oversight, and then an intelligence scholar—has summarized, "The purpose of these new arrangements was to prevent a further erosion of American liberties at the hands of the intelligence agencies."[293]

Congressional disclosure has not in practice fulfilled these hopes. New disclosure norms have indeed shifted information, power, and political risk to the White House and the Congress [294] (although the mandate,

---

[291] II CHURCH COMMITTEE REPORT, *supra* note 20, at 278.

[292] *Id.* at 293 (citing Madison, Federalist 51 "If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would he necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself. A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions.").

[293] Loch K. Johnson, *Establishment of Modern Intelligence Accountability*, in U.S. NATIONAL SECURITY, INTELLIGENCE AND DEMOCRACY: FROM THE CHURCH COMMITTEE TO THE WAR ON TERROR 37, 42 (Russell A. Miller ed. 2008).

[294] *See, e.g.*, Loch K. Johnson, *Ostriches, Cheerleaders, Skeptics, and Guardians: Role Selection by Congressional Intelligence Overseers*, 28 SAIS REVIEW OF INTERNATIONAL

operative since 1980, that the Intelligence Community "keep the congressional intelligence committees fully and currently informed of all intelligence activities, other than a covert action"[295] has not always been scrupulously honored). But obstacles to development of legislative expertise and the ordinarily low political salience of intelligence—both themselves rooted in secrecy—have meant that congressional interventions have not played much of a civil-liberties-protective role.[296] Only once, in 1994, has a statute unambiguously increased procedural protections against surveillance—and that amendment was passed in large part to shore up executive authority.[297] By contrast, the executive branch has been able, several times, to elicit congressional acquiescence for statutes to *expand* surveillance authority—the USA PATRIOT Act, the Protect America Act,

---

AFFAIRS 93 (2008); Loch K. Johnson, *The CIA and the Question of Accountability*, 12 INTELLIGENCE AND NATIONAL SECURITY 178 (2014). I do not mean to take much of a position on the longstanding argument about whether the current degree of legislative oversight is adequate, only to argue that intelligence oversight reform promoted disclosure as one of its principal reforms, and has succeeded in achieving, at least, more such disclosure.

[295] National Security Act, 50 U.S.C. § 413a(a)(1) (1947). This provision was inserted into the Act by Pub. L. No. 96-450, § 501(a), 94 Stat. 1975, 1981 (1980).

[296] Others have written at length about the institutional dynamics that undermine effective congressional intelligence oversight, not just of civil liberties but of intelligence policy more generally. As Amy Zegart summarizes her own findings:

> Congress has collectively and persistently tied its own hands in intelligence oversight for a very long time. Two institutional weaknesses are paramount: rules, procedures, and practices that have hindered the development of *legislative expertise* in intelligence, and committee jurisdictions and policies that have fragmented Congress's *budgetary power* over executive branch intelligence agencies. . . . Ten years after 9/11, the United States has an intelligence oversight system that is well-designed to serve the re-election interests of individual legislators and protect congressional committee prerogatives, but poorly designed to serve the national interest.

AMY B. ZEGART, EYES ON SPIES: CONGRESS AND THE UNITED STATES INTELLIGENCE COMMUNITY 10–11 (2011). *See also, e.g.*, L. BRITT SNYDER, THE AGENCY AND THE HILL: CIA'S RELATIONSHIP WITH CONGRESS 1946–2004 (2008); Kathleen Clark, *Congress's Right to Counsel in Intelligence Oversight*, 2011 U. ILL. L. REV. 915 (2011) (observing that congressional oversight has frequently been hobbled by administration insistence that information be shared only with members, not their staff, even staff with appropriate security clearances).

[297] Counterintelligence and Security Enhancements Act of 1994, Pub. L. No.103-359 (1994), 108 Stat. 3454, Sec. 9 (authorizing FISA judges to allow secret physical searches within the United States of "the premises, property, information, or material of a foreign power or an agent of a foreign power for the purpose of collecting foreign intelligence information"); this amendment to FISA substituted FISA Court process for the prior (rare) practice of Attorney General authorization of such searches. *See* MCGEE & DUFFY, MAIN JUSTICE, *supra* note 34, at 342–343; *Warrantless Physical Searches Conducted in the U.S. for Foreign Service: Statement before the Permanent Select Comm. on Intelligence H.R.* (July 14, 1994), http://perma.cc/8D4G-7G2Z (statement of Jamie S. Gorelick, Deputy Attorney General).

and the FISA Amendments Act.[298] (The last of these included some protections along with the expansion of authority.[299]) It is possible that the Snowden disclosures have shifted the political economy enough for Congress to pass a rights-protective measure in response, but the current prospects of serious legislated reform are dim and getting dimmer.[300] .

Thus whatever the Church Committee's ambitions or expectations for their congressional successors, congressional disclosure has increased intelligence accountability but has not so far provided an impetus for responsive additional civil liberties protections. The civil liberties gap left by the limited ambit of constitutional law, and of FISA, remains. Present efforts in Congress to update the surveillance rules to be more liberty-protective in the era of big data may succeed and align "can" with the reformers' ideas about "should"—for a while and for high-salience issues. But even if this happens, it is inevitable that for issues that have not made it into the press, or for issues in the future, there will always be a disjunction between what is legal and what even members of Congress themselves would find to be, on full and public consideration, appropriate policy. Areas of surveillance practice that have not so far leaked—or in which executive practice changes—will remain, and so, concomitantly, will at least some civil liberties gap.

3. Executive Order

Efforts to implement most of the Church Committee's substantive recommendations as statutory law failed; they entered American law instead as part of Executive Order 12,333. As already quoted, the Executive Order does expressly state (in language unchanged from its 1981 promulgation): "Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests."[301] That is, one of 12,333's purposes is to fill the civil liberties gap left by constitutional and statutory law.

But 12,333 cannot live up to that goal. For one thing, the rules' status as part of an executive order renders them both less visible and more easily weakened. The 2008 amendments to 12,333, for example, for the first time allowed inter-agency sharing of signals intelligence "for purposes of allowing the recipient agency to determine whether the information is

---

[298] USA PATRIOT Act, Pub. L. No. 107-56, 272 Stat. 115 (2001); Protect America Act, Pub. L. 110-55, 121 Stat. 552 (2007); FISA Amendments Act, Pub. L. No. 110-261, 2436 Stat. 122 (2008).

[299] *See id.* (implementing limited court supervision for targeted foreign surveillance, mostly for the first time).

[300] *See* Spencer Ackerman, *Senate Republicans Block USA Freedom Act Surveillance Reform Bill*, THE GUARDIAN (Nov. 19, 2014), http://perma.cc/BVG3-V4Q9.

[301] Exec. Order No. 12,333 § 2.2.

relevant to its responsibilities and can be retained by it," pursuant to potential "procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General."[302] This change received no attention by non-governmental commentators.[303]

More important, even if Executive Order 12,333 adequately covered civil liberties interests in 1980, it—along with its associated AG Guidelines—has grown out-of-date in subsequent decades. Unsurprisingly, given the generally low visibility of intelligence matters, there was little appetite to update either Executive Order 12,333 or other sources of executive self-regulation to address new challenges to liberty, until the Snowden disclosures. Thus notwithstanding the enormous changes that have taken place in the scope of surveillance since 1980 and the advent of "big data" methods, there have been no substantive liberty-protective changes ever made to the Executive Order. Some procedural protections have been added,[304] and notable efforts to *weaken* the protection of U.S. Person information were fended off.[305] But whatever further substantive protection might be useful in light of technological or other changes, all that has been added since 1980 is new hortatory language swearing fealty to (already binding) other laws: "The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law."[306]

Of course, in the rare situation of important disclosures, public discontent about surveillance practices might prompt the President to update Executive Order 12,333, as public discontent has occasionally prompted

---

[302] *Compare* Exec. Order No. 12,333 § 2.3(j), *amended by* Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008), *with* Exec. Order No. 12,333 § 2.3, 46 Fed. Reg. 59941 (Dec. 4, 1981); *see also* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CIVIL LIBERTIES AND PRIVACY OFFICE, CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE 2008 REVISION OF EXECUTIVE ORDER 12333 [hereinafter CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER], http://perma.cc/7WEV-FJAP. No such procedures have been released.

[303] More recently, Emptywheel has analyzed this and other changes. *See, e.g.*, *2008's New and Improved EO 12333: Sharing SIGINT*, EMPTYWHEEL (Feb. 28, 2014), https://perma.cc/S5QK-R2VU.

[304] In adding the Director of National Intelligence to the Executive Order, the 2008 amendments did implicitly incorporate the role of the Civil Liberties Protection Officer, who reports to the DNI. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638; Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008); CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER, *supra* note 302. In addition, the 2008 amendments called for several new procedures, to be approved by the Attorney General.

[305] PROGRAM MANAGER, INFO. SHARING ENV'T, FEASIBILITY: REPORT FOR THE CONGRESS OF THE UNITED STATES (2008), http://perma.cc/B8F5-XXC2.

[306] Exec. Order 12,333 § 1.1(b) (as amended by Executive Order 13470, 73 Fed. Reg. 45325).

other policies that back away from the edge of lawfulness.[307] Indeed, the January 17 promulgation of PPD-28 is a step in this direction. In addition to directing the development of policies to give foreigners some of the same protections already available to U.S. persons,[308] PPD-28 includes some new civil liberties—and even civil rights—protective language:

> "Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[309]

> "Signals intelligence activities shall be as tailored as feasible."[310]

> "In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent [or] disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion . . . ."[311]

PPD-28's new language related to "purpose" is limited in its bite (like any sole purpose requirement). It is, however, susceptible to implementation under a compliance framework. One can imagine a compliance regime that requires documentation and audit of the purpose of SIGINT collection, or of the use of information collected in bulk, to ensure that those purposes are not "suppressing or burdening criticism or dissent," or "disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion." But the other language quoted above reveals a very different, supplemental, approach. Making "privacy and civil liberties . . . integral considerations in the planning of U.S. signals intelligence activities," and ensuring that "[s]ignals intelligence activities . . . [are] as tailored as feasible" are not compliance tasks; they are policy tasks. PPD-28, like several other recent reform proposals, is thus adding to the existing intelligence legalism regime a distinct concept of non-legalistic internal bureaucratic measures—a liberty-protective infrastructure that can put civil liberties concerns into the policy mix, asking the "should" question. This is a new development. Previously, the compliance mindset within the Executive branch has failed to

---

[307] Consider along these lines, for example, the FBI's Attorney General Guidelines and Domestic Investigations and Operations Guide (DIOG). For the history of these documents, see, *e.g.*, Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. 3, 13 (2014).

[308] PPD-28, *supra* note 224, §§ 2-4.

[309] *Id*. § 1(b).

[310] *Id*. § 1(d).

[311] *Id*. § 2.

encourage—and even discouraged—policy-based consideration of civil liberties, for reasons I now explore.

B. Lawyers Are Not Civil Libertarians

Within a particular organization such as the NSA, the impact of a rights and compliance frame is to allocate decision-making to lawyers. If those lawyers have a civil libertarian orientation, this could be a channel by which rights and compliance serve civil liberties interests. That is, one could imagine that agency lawyers might systematically exercise a pro-liberty orientation, which could fill gaps that might otherwise exist. However, multiplying accounts of lawyers in the Intelligence Community suggest otherwise. A growing shelf-full of articles and books document and even celebrate the lawyers who now populate the military, the CIA, and the Department of Justice's National Security Division. Jack Goldsmith, for example, has labeled these lawyers a key part of "something new and remarkable," describing "giant distributed networks of lawyers, investigators, and auditors, both inside and outside the executive branch, that rendered U.S. fighting forces and intelligence services more transparent than ever, and that enforced legal and political constraints, small and large, against them."[312] Might all these lawyers push the intelligence enterprise towards appropriate balancing of liberty and security, even in the absence of specific law or doctrine declaring the required outcome?

I think not. Rather, when lawyers (in an office where they are understood to be practicing law) are given policy roles, those lawyers' legal sign-off frequently stands in as sufficient justification to undertake the policy. To quote Goldsmith one last time, describing the Bush administration's aggressive stance on a variety of national security topics, the role of lawyers was part of why "'What should we do?' . . . often collapsed into 'What can we lawfully do?'"[313] The emerging evidence suggests that national security agency counsel are implementers of two major sets of values—fiduciary/counselor, and rule of law—but not civil liberties. Judge James E. Baker's book-long defense and explication of the role of lawyers in the national security state barely mentions the key civil liberties values of freedom of speech or religion, the right to travel, or due process, but repeatedly emphasizes the centrality of building "a society and a government bound by law, and respect for law."[314] Consider one last time that 2005 speech to the NSA's lawyers and their colleagues, by then-Deputy Attorney General James Comey, in which he praised the NSA's lawyers as "custodian[s] of our constitution and the rule of law." Comey did not exhort his audience of intelligence lawyers to ask the "should" question, rather than

---

[312] GOLDSMITH, POWER AND CONSTRAINT, *supra* note 34, at xi-xii.

[313] GOLDSMITH, THE TERROR PRESIDENCY, *supra* note 34, at 131.

[314] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 21 (2007).

the "can" question. Rather, the commitment he attempted to bolster was to legal compliance, not to individual liberty. To quote his revealing phrase again, he pleaded for "'yes' when it can be, . . . 'no' when it must be."[315]

And as I pointed out in this article's introduction, the "no's" Comey praises may make remarkably little difference, in the end. The hospital-bed confrontation leading to the brief shut-down of part of the "President's Surveillance Program"—the modern ur-episode of intelligence legalism—is a perfect case in point. Lawyers, it seems to me, are far more likely to move an organization towards this kind of nearly symbolic compliance than to effect any more significant constraint on executive activity, particularly with respect to a program important to the President. Indeed, lawyers are attractive to intelligence organizations because they are simultaneously able to give agency operations an imprimatur of lawfulness and to maintain their agency affiliation/loyalty.[316] Their occasional "no's," which like as not have formal rather than major substantive effects, are a price worth paying for those traits.

C. The Costs of Intelligence Legalism

Theorists and observers in a variety of fields have developed the broad critique that law and its concomitant rights orientation may have the counterintuitive impact of decreasing the welfare of the purported rights holders—or, in a more modest version of the point, may ameliorate some prevalent set of harms but undermine more ambitious efforts. Focusing particularly on litigation, they argue that it is inherently a timid enterprise, and yet it crowds out other more muscular approaches.[317] Even with respect to out-of-court rights orientation, or "legalization," scholars have offered the insight that formalizing/legalistic approaches can come with real costs to their intended beneficiaries, depending on the context.[318] The issue is

---

[315] Comey, *supra* note 4.

[316] *Cf.* Rosa Brooks, *The Man Who Knew Too Little*, AMERICAN PROSPECT (Jan. 14, 2014), http://perma.cc/7Z74-P47U (describing the CIA's general counsel's self-reported involvement in all Agency affairs, and noting, "A cynic might suggest that Clarridge's willingness to seek legal guidance was fueled by his confidence that Rizzo would never provide an answer he didn't like").

[317] *See, e.g.*, DUNCAN KENNEDY, A CRITIQUE OF ADJUDICATION (FIN DE SIÈCLE) 300–04, 315–37 (1997) (setting out an intellectual history of the critique of rights); Alan Freeman, *Racism, Rights and the Quest for Equality of Opportunity: A Critical Legal Essay*, 23 HARV. C.R.-C.L. L. REV. 295, 296 (1988) (describing the rights discourse employed in the development of antidiscrimination law as "a process of containing and stabilizing the aspirations of the oppressed"). On the other hand, for discussions of how litigation and litigation victories can be converted into useful political currency, see MICHAEL MCCANN, RIGHTS AT WORK: PAY EQUITY REFORM AND THE POLITICS OF LEGAL MOBILIZATION (1994); STUART A. SCHEINGOLD, THE POLITICS OF RIGHTS (1974); CHARLES R. EPP, MAKING RIGHTS REAL: ACTIVISTS, BUREAUCRATS, AND THE CREATION OF THE LEGALISTIC STATE (2009).

[318] *See, e.g.*, William H. Simon, *Legality, Bureaucracy, and Class in the Welfare System*, 92 YALE L.J. 1198, 1231 (1983) ("The transformation of the system has increased its accessibility and responsiveness to people with rule knowledge and enforcement resources,

whether, in a particular institutional setting, these possibilities have materialized. In this Section, I examine two pathways by which intelligence legalism tends to impair the prospects of a softer civil-liberties protective policy.

1. Intelligence Legalism Crowds Out Interest Balancing

This Article demonstrates the high salience of rights in this realm. Several related mechanisms convert that high salience into a devaluation of interests:

First, rights occupy the "liberty" field because of the practical issue of attention bandwidth, which potentially applies both to agencies and advocates. After all, even large organizations have limited capacity.[319] NSA compliance is such an enormous task that little room remains for more conceptual weighing of interests and options. Recall that of the dozen-plus offices I described in Part II, just two—the Civil Liberties and Privacy Office at the NSA, and the Privacy and Civil Liberties Oversight Board—are currently playing a policy rather than strictly a compliance role. They are also, not coincidentally, the two newest and two smallest of the offices listed.

I think, though, that this bandwidth issue is driven by a more conceptual, less practical, factor: that rights talk hides the necessity of policy judgments and, by its purity, diverts attention from that messier field. Morton Horwitz explains the point:

> A . . . troubling aspect of rights discourse is that its focus on fundamental, inherent, inalienable or natural rights is a way of obscuring or distorting the reality of the social construction of rights and duties. It shifts discussion away from the always disputable issue of what is or is not socially desirable. Rights discourse . . . wishes us to believe instead that the recognition of rights is not a question of social choice at all, as if in the normative and constitutional realm rights have the same force as the law of gravity.[320]

---

in particular professional advocates. But very few recipients have the knowledge and resources of professional advocates and only a few more are able to get representation by professional advocates. For the rest, formalization and bureaucratization have in many ways decreased accessibility and responsiveness.").

[319] *See, e.g.*, James G. March & Herbert A. Simon, Organizations (1958). *See also* RICHARD THOMPSON FORD, RIGHTS GONE WRONG: HOW LAW CORRUPTS THE STRUGGLE FOR EQUALITY 25 (2011) ("Those working for social justice all too often eschew the difficult and unpleasant task of popular persuasion, lured by the false hope of a shortcut by way of judicially mandated civil rights. And even policy reform pursued through the democratic process often takes the form of new civil rights.").

[320] Morton Horwitz, *Rights*, 23 HARV. C.R.-C.L. L. REV. 393, 403–04 (1988).

Mary Dudziak makes a similar claim in her recent discussion of law and drone warfare, "In this context, law . . . does not aid judgment, but diverts our attention from morality, diplomacy, humanity, and responsibility in the use of force, and especially from the bloody mess left on the ground."[321]

Even in Fourth Amendment jurisprudence, an area of constitutional doctrine explicitly imbued with policy considerations, we talk about rights as if they are somehow scientific, to be deduced rather than debated. The discussion that must accompany policy claims pales in prestige and importance by comparison. And from the perspective of their beneficiaries, judicially enforceable rights, with their promise of supremacy over competing interests, are shiny and magnetic. This is why the assertion of rights can be such a powerful organizing tool[322]—even if those rights don't turn out to change much on the ground. As Rich Ford has written, "Rights are a secular religion for many Americans."[323] Or to quote Alan Freeman's classic article about civil rights, "Rights consciousness can offer sustenance to a political movement, however alienated, indeterminate or reified rights may be."[324]

It is the purity, the apparent apolitical nature, of rights that makes them nearly the only coin available. By comparison with judicially enforceable rights, other methods of advancing individual liberty look feeble, contingent, jury-rigged. An accusation of illegality becomes the required first bid for any policy discussion, and a refutation of that accusation ends play. This dynamic is very much in evidence in the response to the PCLOB's 702 report, described above. Rights discourse stunts needed policy discourse.[325]

2. Intelligence Legalism and Legitimation

In addition, judicial review legitimates the American surveillance system; that is why reference to court supervision is surveillance proponents' first recourse when they want to suggest that everything is fine. It is, for example, a rare speech by a government official that fails to make reference to the FISA Court and its ratification of the government's surveillance

---

[321] Mary L. Dudziak, *Nations United?*, DEMOCRACY, Winter 2013, http://perma.cc/S6ZU-ASW7.

[322] *See* MCCANN, *supra* note 317; SCHEINGOLD, *supra* note 317; EPP, *supra* note 317.

[323] FORD, *supra* note 319, at 19.

[324] Freeman, *Racism, Rights*, *supra* note 317, at 333 n.99 (citing Peter Gabel, *The Phenomenology of Rights-Consciousness and the Pact of the Withdrawn Selves*, 62 TEX. L. REV. 1563, 1588–89 (1984)).

[325] This is akin to some of the effects of administrative law on allocation of power within federal agencies between lawyers and experts. *See* Elizabeth Magill & Adrian Vermeule, *Allocating Power Within Agencies*, 120 YALE L.J. 1032 (2011).

programs. Below are passages, chosen essentially at random, from a speech by President Obama on the topic of signals intelligence reform[326]:

- "I ordered that our programs be reviewed by my national security team and our lawyers . . . . We increased oversight and auditing, including new structures aimed at compliance. Improved rules were proposed by the government and approved by the Foreign Intelligence Surveillance Court."
- "[T]he Foreign Intelligence Surveillance Court . . . provides judicial review of some of our most sensitive intelligence activities."

In language like the above, court involvement is offered as evidence of both legality and appropriateness; indeed, the two are conceptually merged.

My point is not that FISA Court legitimation is phony. In fact, judicial review has real effects on the system—we know from the recently declassified documents that FISA Court review disciplines the surveillance system, holding it at least to the government's own representations.[327] Yet the oversight gain carries with it a legitimation cost; the existence of judicial review makes political change more difficult. Scholars, particularly critical legal studies scholars, have made this point in a large number of other contexts. For example, Alan Freeman argued that civil rights law—and law more generally—exists "largely to legitimize the existing social structure."[328] The polity at large is soothed, and the effect is felt even by rights beneficiaries, who frame and tame their aspirations to suit the inherently limited scope of potential judicial interventions. Freeman described his view that American civil rights litigation has amounted to a "process of containing and stabilizing the aspirations of the oppressed through tokenism and formal gestures which actually enhance the material lives of few."[329] He wrote:

> Rights are granted to, or bestowed upon, the powerless by the powerful. They are ultimately within the control of those with authority to interpret or rewrite the sacred texts from which they derive. To enjoy them, one must respect the forms and norms laid down by those in power. One must especially avoid excesses in behavior or demands.[330]

---

[326] Press Release, *Remarks by the President on Review of Signals Intelligence* (Jan. 17, 2014), http://perma.cc/9J72-4EGU.

[327] *See, e.g.*, Bates, Memorandum Opinion (July 2010), http://www.clearinghouse.net/chDocs/public/NS-DC-0030-0001.pdf [http://perma.cc/2CFL-ZF2J].

[328] Alan Freeman, *Legitimizing Racial Discrimination Through Antidiscrimination Law: A Critical Review of Supreme Court Doctrine*, 62 MINN. L. REV. 1049, 1051 (1978).

[329] Freeman, *Racism, Rights*, *supra* note 317, at 296.

[330] *Id.* at 331.

The point is not, for Freeman (and the plentiful literature he adduced), that law accomplishes nothing for its purported beneficiaries. If that were true, it could not legitimate: "[I]f law is to serve its legitimation function, [the] ultimate constraints [that come from politics] must yield up just enough autonomy to the legal system to make its operations credible for those whose allegiance it seeks as well as those whose self-interest it rationalizes."[331] But gains from rights may—and in the surveillance situation clearly do—make gains from politics less available.

To sum up this Part, neither the Constitution nor FISA aims to optimally balance security and liberty—and frequently analyzed difficulties in congressional intelligence oversight mean that new statutes are unlikely to fill that gap. Likewise the existing foundational Executive Order, 12,333, is at the very least out-of-date. Accordingly intelligence legalism, and its compliance mindset, cannot achieve optimal policy. Its concomitant empowerment of lawyers is real and important, but does not deputize a pro-civil liberties force. Indeed, legalism actually both crowds out the consideration of policy and interests (as opposed to law and rights), and legitimates the surveillance state, making it less susceptible to policy reform. Are there, then, non-legalistic reforms that could play a productive part? I turn next to this issue.

IV. Reforms

Since the Guardian's PRISM story in June 2013, dozens of specific reforms have been proposed for the NSA and the FISA court. Bill after bill was introduced in the Congress; though none were enacted, one even passed in the House.[332] The President appointed a blue-ribbon "Review Group on Intelligence and Communications Technologies," which after just five months of work offered him 46 recommendations.[333] The Privacy and Civil Liberties Oversight Board issued its first two reports, with 22 recommendations between them.[334] Advocacy organizations have weighed in, as have blogging scholars, former government officials, and journalists and newspaper editorial boards. The President himself has responded by

---

[331] Freeman, *Legitimizing Racial Discrimination*, *supra* note 328, at 1051.

[332] H.R. 3361 (113th Cong.) (as passed by House, May 22, 2014). For other examples of proposed NSA-reform legislation, see: S. 2685 (113th Cong.) (Senator Leahy's proposed USA Freedom Act; cloture motion failed Nov. 18, 2014); S. 1631 (113th Cong.) (as referred to the S. Select Comm. on Intelligence, Oct. 31, 2013); H.R. 3436 (113th Cong.) (as referred to H.R. Comm. on Intelligence, Oct. 30, 2013); S. 1551 (113th Cong.) (as referred to S. Comm. on the Judiciary, Sept 25, 2013); H.R. 2399 (113th Cong.) (as referred to H.R. Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations); S. 1130 (113th Cong.) (as referred to S. Comm. on the Judiciary, June 11, 2013); S. 1121 (113th Cong.) (as introduced in Senate, June 7, 2013).

[333] *Liberty and Security in a Changing World: Report and Recommendations*, PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (Dec. 12, 2013) [hereinafter REVIEW GROUP REPORT], http://perma.cc/ZM54-5T8Y.

[334] PCLOB, 215 REPORT, *supra* note 246; PCLOB, 702 REPORT, *supra* note 258.

announcing a number of reforms, and a process to evaluate others, as well as promulgating a significant new Presidential Policy Directive.

The reforms proposed and announced nearly all cluster into one or more of eight categories:

- Deepen surveillance legalism and skepticism towards bulk or wholesale data collection, by eliminating it, or in the alternative by imposing more court oversight, tighter government access to surveillance results, more-individuated showings of need.[335]
- Increase public disclosure.[336]
- Raise the level of governmental review for a variety of sensitive decisions.[337]
- Treat foreigners abroad more like (but not just like) U.S. persons.[338]
- Shrink the NSA's ambit and perhaps even demilitarize it somewhat.[339]
- Support global internet openness and security.[340]
- Improve personnel and network security.[341]
- Create/strengthen governmental offices and procedures directed at privacy and civil liberties.[342]

Much of the reform action is, and should be, devoted to substantive interventions. Congress should itself ask the "should" question, and can insist on, for example, tighter rules governing bulk collection, requiring more-individuated justifications for data acquisition, analysis, and use. Or to rephrase the point using the familiar vocabulary of rules and standards,[343]

---

[335] *E.g.*, REVIEW GROUP REPORT, *supra* note 333, recommendations 1, 2, 3, 4, 5, 12, 20; PCLOB, 215 REPORT, *supra* note 246, recommendations 1, 2; PCLOB, 702 REPORT, *supra* note 258, recommendations 1–7, 9; USA FREEDOM Act, S. 2685, 113th Cong. (2013–2014), § 101.

[336] *E.g.*, REVIEW GROUP REPORT, *supra* note 333, recommendations 7, 8, 9, 10, 11, 28; PCLOB, 215 REPORT, *supra* note 246, recommendations 5, 6, 7, 8, 9, 11, 12; PCLOB, 702 Report, *supra* note 258, recommendations 8, 9.

[337] *E.g.*, REVIEW GROUP REPORT, *supra* note 333, recommendations 11, 16, 17, 18, 30, 44; PCLOB, 215 REPORT, *supra* note 246, recommendations 4, 10.

[338] *E.g.*, REVIEW GROUP REPORT, *supra* note 333, recommendations 19, 21.

[339] *E.g.*, *id.*, recommendations 22, 23, 24, 25.

[340] *E.g.*, *id.*, recommendations 29, 30, 31, 32, 33.

[341] *E.g.*, *id.*, recommendations 37, 38, 39, 40, 41, 42, 43, 44, 45, 46.

[342] *E.g.*, *id.*, recommendations 26, 27, 28, 35, 36; PCLOB, 215 REPORT, *supra* note 246, recommendations 3, 5, 8, 10; USA FREEDOM Act, S. 2685, 113th Cong. §§ 401, 504 (2013–2014).

[343] *See, e.g.*, Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Kathleen M. Sullivan, *The Supreme Court, 1991 Term—Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22 (1992).

Congress, and the President, can design and promulgate new rules to serve the overarching standard—that liberty should be prioritized where it carries no, or acceptable, cost to security—and these rules can then be enforced by a compliance regime.

But what about implementation of the underlying standard itself: the idea that liberty should be prioritized where it carries no, or acceptable, cost to security? I argued in Part III that surveillance secrecy and the very significant changes over time mean that some opportunities to further that standard are likely to remain untouched by the Constitution, statutes, and executive order. So while I am far from opposed to additional statutory and regulatory-type rules, there remains an additional opportunity to further individual liberty and privacy with less legalistic, more standard-like interventions. This opportunity is the thrust of the last category of reforms, which propose to institutionalize within the Executive branch, the question of "should" rather than "can":

- The President announced in August 2013 that the NSA would "put in place a full-time civil liberties and privacy officer."[344] The job announcement went up in September,[345] and as already described, the new NSA Civil Liberties and Privacy Officer, Rebecca Richards, began work in January.[346]
- The President's Review Group also recommended "the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget."[347] The President has agreed; this is included in PPD-28,[348] and several White House staffers are now assigned to this role, including one each at the Office of Management and Budget, National Security Council staff, and the Office of Science and Technology Policy. [349]
- The President's Review Group delved further into the type of work product that would promote consideration of privacy and civil liberties, recommending that the government use Privacy and Civil Liberties Impact Assessments for "big data and data-mining programs directed at communications," in order to ensure that such efforts are statistically reliable, cost-effective, and

[344] Press Release, President Barack Obama, Remarks by the President in a Press Conference (Aug. 9, 2013), http://perma.cc/GB8K-6DJE.

[345] Moyer, *supra* note 119.

[346] Richards Interview, *supra* note 15.

[347] REVIEW GROUP REPORT, *supra* note 333, recommendation 26.

[348] PPD-28, *supra* note 224. The "new privacy officer" is assigned two tasks related to DNI oversight in a "disclosures action tracker" used by White House staff to manage deadlines and progress on proposed and promised surveillance reforms. *Draft: Disclosure Action Tracker* (Jan 25, 2015, 9:16 PM), http://perma.cc/8D5U-5RST.

[349] White House Official Interview, *supra* note 15. Counselor to the President John Podesta also plays a role. *Id.*

protective of privacy and civil liberties.[350] NSA's new Civil Liberties and Privacy Office is working through how to conduct assessments along these lines.[351]

- The President's Review Group also recommended that "program reviews" be instituted, external to the IC elements in question, "to assess and respond to emerging privacy and civil liberties issues"; these might be done by the PCLOB or some other way.[352] The USA Freedom Act, the leading reform bill—which though it died in the Senate, will likely be the starting point for any congressional intervention in 2015—would have required the Intelligence Community Inspector General to do a similar kind of review.[353]
- A reform proposal endorsed by nearly everyone[354] (with some cavil by former FISA presiding Judge John Bates[355]) is to adjust FISA proceedings by introducing some kind of public advocate with a systematic role. In the President's Review Group formulation: create a "Public Interest Advocate to represent privacy and civil liberties interests" in the FISA Court, allowing the Court to invite participation, but also allowing the Advocate to "intervene on her own initiative."[356] The President agreed, "calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court."[357] This was included in the Senate version of the USA Freedom Act.[358]
- The PCLOB, in its report on 702 surveillance, urged the government to "develop a comprehensive methodology for

---

[350] REVIEW GROUP REPORT, *supra* note 333, recommendation 35.

[351] Richards Interview, *supra* note 15.

[352] REVIEW GROUP REPORT, *supra* note 333, recommendation 36.

[353] USA FREEDOM Act, S. 2685, 113th Cong. (2013-2014), § 108.

[354] PCLOB, 215 REPORT, *supra* note 246, at 183 (recommendation 3); REVIEW GROUP REPORT, *supra* note 333, recommendation 28; USA FREEDOM Act, S. 2685, 113th Cong. § 401 (2013–2014); President Barack Obama, Remarks by the President on Review of Signals Intelligence, *supra* note 326.

[355] Letter from Judge John D. Bates, Director of the Administrative Office of the United States Courts, to Senator Dianne Feinstein, Chairman, Senate Intelligence Committee (Jan. 13, 2014) [hereinafter Bates-Feinstein letter], http://perma.cc/T9TN-AQWM; *see also* Letter from John D. Bates, Director of the Administrative Office of the United States Courts, to Senator Patrick J. Leahy, Chairman, Committee on the Judiciary (Aug. 5, 2014) [hereinafter Bates-Leahy letter], http://perma.cc/49PB-MZNU; John D. Bates, *Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act* (Jan. 10, 2014) [hereinafter Bates, *Comments on FISA Proposals*], http://perma.cc/5UJC-DH85; H.R. REP. NO. 113-452, at 41–43, https://perma.cc/2WZG-QVQQ (including letter from John D. Bates to Congressman Mike Rogers).

[356] PCLOB, 215 REPORT, *supra* note 246, at 204.

[357] President Barack Obama, Remarks by the President on Review of Signals Intelligence, *supra* note 326.

[358] USA FREEDOM Act of 2014, S. 2685, 113th Cong. § 401 (2013–2014).

> assessing the efficacy and relative value of counterterrorism programs," in order to effectively weigh the interests of the government in conducting a program against the intrusions on privacy and civil liberties that it may cause."[359]

Each of these proposals would designate either an office, person, or process to prioritize privacy and civil liberties—values that, as we have seen, otherwise lack advocates within the NSA's governance structure. So might they really change anything at the NSA? I next look at three new/proposed offices.

I have suggested that rights discourse tends to sweep under the rug the messiness of civil liberties protections—the policy issues that lie at the core of civil liberties interests. That messiness will be apparent in what follows; there are no magic bullets here. But a measure can be useful even if messy or compromised. It is possible that that none of the offices described below will accomplish very much. It seems to me, however, that soft administrative measures are useful tools in the civil liberties toolkit, well worth trying by a principal—whether that principal is the President or the Congress—who wants to give more priority to civil liberties but lacks the institutional capacity to do so directly and repeatedly over time. Each of these three offices *might* represent civil liberties interests more systematically than current arrangements, and might advocate for more liberty protective government protocols and programs. It is worth emphasizing, too, that measures such as these might have not just cumulative but also mutually reinforcing effects, creating a civil liberties cadre with security clearances, who might assist each other in a variety of ways.[360] In addition to promoting civil liberties/privacy interstitially, offices like these assist other more authoritative rulemakers to understand the civil liberties implications of their choices. For example, they can help Congress in its otherwise very difficult oversight task, flagging issues that need more congressional attention.[361] And in several different ways, they may increase public access to otherwise secret matters, which in turn increases pressure on those authoritative rulemakers: They generate reports—both public and private—which can be used by Congress and the public.[362] And they build relationships with non-governmental organizations that promote increased official disclosure. My argument is not that offices like these are a cure-all

---

[359] PCLOB, 702 REPORT, *supra* note 258, at 148.

[360] *Cf.* ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 81 (2008) (describing the influential role of national privacy authorities in creating a European pro-privacy regulatory regime; domestic authorities built powerful networks both within their own countries and transnationally).

[361] This kind of office can serve a congressional "fire-alarm" oversight strategy. *See* Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols versus Fire Alarms*, 28 AM. J. POL. SCI. 165 (1984).

[362] Consider, along these lines, Ben Wittes's 2008 writing about the importance of "a body of material—public and classified—that enables ongoing debate as to whether the counterterrorism bang of a given surveillance tactic or policy is worth its civil liberties buck." WITTES, LAW AND THE LONG WAR, *supra* note 47, at 253.

for achieving optimal policy, but that they may be a useful part of a complicated ecology.

A. NSA Office of Civil Liberties and Privacy

I describe the NSA's new Office of Civil Liberties and Privacy above in Section II.A. Here I ask what steps might maximize the chances that the office could succeed, or at least make a real impact. The twin dangers of impotence and capture/assimilation threaten all such Offices of Goodness.[363] The extraordinarily high stakes of counterterrorism work increase both dangers at NSA: nobody wants to be the person whose prioritization of liberty led to someone's death. And yet both could be ameliorated by certain organizational choices:

1. Maintaining Influence

Any internal office whose mission is to constrain its agency runs the risk of losing influence and being ignored, whether by being excluded from working groups and processes or by having its attempted contributions rebuffed. This dynamic might be particularly strong at the NSA, because internal actors have up until now identified compliance problems as the threat to privacy/civil liberties. If the NSA's new civil liberties office is going to add anything distinctive, it will need to embrace interests rather than rights, policy rather than compliance. But as discussed above, the attraction of the compliance frame is the legitimation it provides. When the new office takes on policy tasks, lacking that legitimation, it will be especially bureaucratically vulnerable to being frozen out.

Moreover, many of the tools usually available to an Office of Goodness to augment its own influence will be unavailable because of the secrecy that surrounds NSA activities. In many circumstances an Office of Goodness asked to publicly ratify particular agency choices (activities, approaches, rules) can pressure agency leadership into making, or shading, certain choices in exchange for that ratification. But the NSA civil liberties office will often be unable to provide publicly-visible ratification, because the programs in question are secret. Accordingly, office leadership will lack that pressure point. Offices of Goodness can often cultivate external advocacy organization support, but the NSA civil liberties office's access to this tool is similarly undermined by secrecy. Offices of Goodness can gain influence by generating documents that then become public, whether because they are officially released, leaked, or turned over because of a Freedom of Information Act or litigation discovery request. But in the classified environment these avenues of communication, too, are extremely narrow, which means that agency flouting of office views is less costly than

[363] Schlanger, *Offices of Goodness*, *supra* note 76, at 103–116.

it would otherwise be.[364] All three of the strategies just mentioned rely on a public constituency to bolster an Office of Goodness's influence—because, as James Q. Wilson summarizes, for federal agencies, "[t]he principal source of power is a constituency."[365] The NSA civil liberties office will have a public constituency, but secrecy cannot but undermine how much help that constituency can provide.

So in order to remain empowered, the NSA civil liberties office will need to cultivate alternative allies, with security clearances—at ODNI, DOJ, at the White House, and in Congress. I imagine this too will be a challenge. Beginning with ODNI and DOJ, the most obvious potential sources of support will be from those agencies' Civil Liberties and Privacy Officers. But neither is able to carry much water. The ODNI civil liberties office, as already described, has chosen to function more as a compliance-type than a policy office. At DOJ, the Civil Liberties and Privacy Office lacks influence over foreign intelligence matters, which are allocated instead to the National Security Division. Indeed, no list of relevant offices or proposal of potential actors to increase oversight of which I'm aware have even mentioned this office.[366] And the National Security Division lawyers are so committed to intelligence legalism, so firmly embedded in a compliance system, that they are unlikely to be very sympathetic to policy arguments that the government *could* but should not undertake some step or activity. Besides, a policy orientation would reduce NSD's influence. Congress is also a somewhat hopeful prospect. But an NSA civil liberties office is unlikely to lean far enough to the left to hold the support of the most vocal congressional critics of the NSA. And yet the most conservative members of the Intelligence Committees are not natural allies either. In addition, all the obstacles to sustained congressional attention to and oversight of intelligence, discussed above, must obstruct fine-gauge interventions that might be useful to the office's influence. In short, the new NSA civil liberties office will be hard pressed to cement the alliances on which, like every Office of Goodness, it will depend for influence. (I discuss the possibility of a White House alliance in the next section.)

The institutional design of the new office should take account of these difficulties in gaining a constituency or allies. The office's mandate

---

[364] I develop the ideas summarized in this paragraph in Schlanger, *Offices of Goodness*, *supra* note 76, at 105–112.

[365] JAMES Q. WILSON, BUREAUCRACY: WHAT GOVERNMENT AGENCIES DO AND WHY THEY DO IT 204 (1989).

[366] Libin Interview, *supra* note 15. On the relative influence of DOJ's Privacy and Civil Liberties office compared to NSD, *see, e.g.*, NSD 2008 PROGRESS REPORT, *supra* note 173, at 22. ("[Compliance reviews] are staffed by NSD attorneys within the Office of Intelligence, working along-side lawyers from the FBI's Office of General Counsel. Additionally, officials from the Department's Privacy and Civil Liberties Office have accompanied some review teams and are briefed on the teams' findings."); *id*. at 23 ("We report to the Attorney General semiannually on findings regarding such referrals [of compliance violations], and inform the Department's Chief Privacy and Civil Liberties Officer of any referral that raises serious civil liberties or privacy issues.").

from the NSA's director should include a stable set of situations in which it can have access to the policy making process, and opportunity to participate, without needing sharper elbows than it is likely to have. The President's Review Group's recommendations about impact assessments are helpful, even vital, in this regard and should, in fact, be substantially expanded. The Review Group report explains that the kind of impact assessment it proposes "should be broader and more policy-based that has usually been the case for PIAs [Privacy Impact Assessments]. For instance, policy officials should explicitly consider the costs and benefits of a program if it unexpectedly becomes public." [367] But the recommendation covers only "the broader programs that may constitute multiple systems." For impact assessments[368] to play the role I am sketching of bolstering the access and influence of an NSA civil liberties office, they would need to be required for more programs.

Other types of institutionalized access might also assist. For example, perhaps the operational offices could be required to report every year to the new civil liberties office how, precisely, each type of surveillance authority that touches U.S. persons has contributed to the NSA's foreign intelligence mission—intelligence requirements satisfied, leads generated, etc. The office could use those reports to do an annual assessment for the NSA's director of costs and benefits of the various programs. Certainly, one would want to ensure that the new office receives notice and an opportunity to comment[369] on all operational changes that potentially impact privacy or civil liberties—that is, that sweep in more data or data for more people, particularly U.S. persons. Institutionalizing these processes—impact assessments, annual reports, clearance inclusion—would protect the new office's access, a prerequisite to influence if not influence itself. That would further legitimate its inquiries and its recommendation role, protecting it from the accusation of self-aggrandizement or what a lawyer might call "officious intermeddling."

There is a danger to all this access, however. The more involvement in decisionmaking the new NSA civil liberties office has—at both staff and leadership levels—the more pressure it will receive to go along, to ratify whatever it is that the operational staff is requesting. Suppose, for example, the NSA civil liberties officer has the power to non-concur in some situation and have that non-concurrence push the issue to NSA's director for decision. Forcing the director to choose between what his operational staff and his civil liberties staff propose is putting him in a no-win situation; the pressure to avoid that will be intense. What counters that pressure, if anything, is the new official's commitment to her assigned values, privacy and civil liberties. I now move to this topic.

---

[367] REVIEW GROUP REPORT, *supra* note 333, at 230.

[368] Schlanger, *Offices of Goodness*, *supra* note 76, at 96–98.

[369] *Id.* at 32.

2. Maintaining Commitment

The NSA's civil liberties office will be able to bolster civil liberties only if its leader and staff stay committed to this "precarious value,"[370] notwithstanding the value's oppositional nature within the NSA. Maintaining commitment means resisting both collegial and careerist pressures, both born of normal desires to get along with colleagues and to earn their approbation. The goal is to avoid a special kind of "capture"—not, as the term usually indicates, by outsiders, but by colleagues. What is needed are careful and multi-pronged efforts to tie NSA civil liberties staff to a professional privacy and civil liberties community that can serve as a highly salient reference group; this should use a combination of hiring, networking, and fostering of career paths that value privacy/civil liberties expertise and commitment.[371] People whose primary professional predilections lean towards civil liberties have both personal and professional incentives to make sure that commitment does not erode. Again, however, the classified setting will make this more difficult than elsewhere. For example, bringing in new employees directly from advocacy groups is a common strategy for Offices of Goodness that seek to ensure staff commitment.[372] But for the NSA civil liberties office, the top secret clearance process can take many months, which puts sharp pressure on hiring managers to hire already-cleared federal employees, not external advocates. Even if civil liberties advocates get hired, they may well run into particularly lengthy clearance investigation delays, based on prior associations, travel, and activities. Office Director Becky Richards reports that five people she has so far brought on board are from within the NSA, to minimize hiring delays (as well as help her get a better understanding of how the NSA works). She has so far hired just one privacy expert from outside the NSA.[373]

Moreover, as I have explained generally about Offices of Goodness staff, "even if they were hired from a Goodness organization, as staff gain experience within the government, that affiliation is likely to fade and their reference group to shift to their more immediate peers."[374] To oppose this shift, an Office's leader can consciously connect its staff to Goodness advocates, for example, by sending them to conferences or other public or private events. This works in two different ways. First, it reinforces Office staff commitment to its assigned value simply by exposure and example. But in addition, outside events can have a disciplining function, penalizing

---

[370] *See* PHILIP SELZNICK, LEADERSHIP IN ADMINISTRATION: A SOCIOLOGICAL INTERPRETATION 119–33 (1957).

[371] Schlanger, *Offices of Goodness*, *supra* note 76, at 112–116.

[372] *See, e.g.*, Kenneth Bamberger & Deirdre Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75 (2008) (account of two federal privacy offices that stresses that hiring staff experienced in the "privacy field" was crucial to the greater success of the DHS office compared to the Department of State office).

[373] Richards Interview, *supra* note 15.

[374] Schlanger, *Offices of Goodness*, *supra* note 76, at 115.

Office capture with harsh questions or criticisms, both public and private. As Sallyanne Payton has written, "[s]tarch for the backbone of weak professional groups generally must come from outside."[375]

Even if the new NSA civil liberties officer expends real attention to situating herself and her staff in networks of privacy and civil liberties advocates, harnessing those networks as reference groups will be difficult to do. Intelligence law professional networks exist—there is a bar association group [376] with conferences, newsletters, and continuing legal education sessions[377]; there are journals,[378] centers,[379] and like markers of professional group-building. Yet none of these is quite on point. As I argued at length above, the shared commitment of members of the national security bar is not to strengthening civil liberties, but rather to technocratic expertise with respect to the very complex legal rules at issue, and perhaps to a strong national security state. At the conferences and in the newsletters, civil liberties get remarkably little attention, although the role of lawyers receives a bit more.[380] It is hard to imagine organizations like the ACLU, Electronic Frontier Foundation, or the Electronic Privacy Information Center (EPIC) embracing full participation in their events by NSA staff.[381] Moreover, as

---

[375] *See* Sallyanne Payton, *[Book review] Elaine Draper, The Company Doctor*, 23 J. POL'Y ANALYSIS & MGMT. 384, 386 (2004).

[376] *About Us*, AMERICAN BAR ASSOCIATION, DIVISION FOR PUBLIC SERVICE, STANDING COMMITTEE ON LAW AND NATIONAL SECURITY, http://perma.cc/T3XD-9MYD (last visited Nov. 17, 2014).

[377] *Events & CLE*, AMERICAN BAR ASSOCIATION, DIVISION FOR PUBLIC SERVICE, STANDING COMMITTEE ON LAW AND NATIONAL SECURITY, http://perma.cc/VV55-4URY (last visited Nov. 17, 2014); Conference, *Past Annual Review Conferences*, AMERICAN BAR ASSOCIATION, DIVISION FOR PUBLIC SERVICE, STANDING COMMITTEE ON LAW AND NATIONAL SECURITY, http://perma.cc/C3ZP-4ZE4 (last visited Nov. 17, 2014).

[378] *See Homepage: National Security Journal*, HARVARD LAW SCHOOL, http://perma.cc/2A5F-C4CL (last visited Aug. 17, 2014); *Homepage: Journal of National Security Law & Policy*, GEORGETOWN LAW & SYRACUSE UNIVERSITY INSTITUTE FOR NATIONAL SECURITY & COUNTERTERRORISM, http://perma.cc/TJA9-BKFZ (last visited Nov. 17, 2014); *Homepage: National Security Law Brief*, AMERICAN UNIVERSITY-WASHINGTON COLLEGE OF LAW, http://perma.cc/4TMD-F3T3 (last visited Nov. 17, 2014); *Homepage: National Security Law Journal*, GEORGE MASON UNIVERSITY SCHOOL OF LAW, http://perma.cc/5DQ5-CLLC (last visited Nov. 17, 2014); *Homepage: National Security & Armed Conflict Review*, MIAMI LAW, http://perma.cc/A3LK-PXAD (last visited Nov. 17, 2014).

[379] *E.g.*, *Homepage: Center for National Security Law*, VIRGINIA SCHOOL OF LAW, http://perma.cc/68DR-R97A (last visited Nov. 17, 2014); *Homepage: The Center on Law, Ethics, and National Security*, DUKE LAW, http://perma.cc/6546-ARR7 (last visited Nov. 17, 2014); *Homepage: Institute for National Security and Counterterrorism*, SYRACUSE UNIVERSITY, http://perma.cc/LN7J-KA79 (last visited Nov. 17, 2014).

[380] *E.g.*, Conference Program, *22nd NSLI Program*, UNIVERSITY OF VIRGINIA SCHOOL OF LAW, CENTER FOR NATIONAL SECURITY LAW (June 1–13, 2014), http://perma.cc/Z7FP-TXMH; Conference Program, *Law Shaping in National Security: The Past, The Progress, and the Path Ahead*, DUKE LAW (Feb. 28–Mar. 1, 2014), http://perma.cc/7ECB-6T2X.

[381] An episode in conference-attendance-gone-wrong played out at Def Con in 2012, when in his keynote address, NSA head Keith Alexander (mis)characterized accusations that the NSA was keeping records on millions of Americans as "absolute nonsense." Federal

always, secrecy makes everything more difficult. The new civil liberties office's staff will not be able to talk much about its work, and that makes them less likely to have their feet held to the civil liberties fire at public events.

A method for avoiding capture that is more promising would use the new NSA civil liberties staff's expectation about their own career paths. If the possibility for career advancement exists chiefly in other NSA jobs, that would be unhelpful; the prod to be a team player and not a constraint would be unduly sharp. (On the other hand, if commitment *could* be maintained, sending civil liberties/privacy staff back into the NSA's operational offices would be a way to seed civil liberties values across the agency.) It will be far easier for the NSA civil liberties office staff to maintain their civil liberties commitment if a sufficient number of national security jobs develop, both within the new office itself and outside, in which demonstrated civil liberties commitment is a prerequisite. Perhaps that will happen; the Snowden disclosures and the natural maturation of this new bureaucratic strategy of civil liberties offices mean that numerous government institutions are gaining civil liberties staff. The PCLOB has a tiny staff, for example, and may well grow. As discussed in the next section, the White House has designated privacy/civil liberties staff. And of course, as the prior discussion makes clear, there are already some such jobs scattered around the government, at ODNI, DOJ, DHS, etc. For example, the new NSA civil liberties officer came from a privacy compliance job at DHS.[382] There are, as well, non-governmental opportunities, as well, at universities, advocacy organizations, etc. The success of the new NSA office and other offices like it may depend on whether this job network reaches critical mass; currently, national security civil liberties jobs within the government are extraordinarily scarce.

In short, to maximize the chances that the new NSA Civil Liberties and Privacy Office will maintain both influence and commitment, the NSA and other government officials should take the following steps:

- Embrace a policy rather than a compliance role for the Office of Civil Liberties and Privacy.
- Foster relationships of Office of Civil Liberties and Privacy staff with civil liberties offices elsewhere throughout the Intelligence Community, with White House personnel, and with Congress.
- Mandate civil liberties impact assessments that assess costs and benefits of surveillance programs.

---

officials were not invited the following year. Jim Finkle, *Hackers Convention Ask Government to Stay Away over Snowden*, REUTERS (July 11, 2013), http://perma.cc/B4LR-7XSU.

[382] *NSA Announces New Civil Liberties and Privacy Officer*, NATIONAL SECURITY AGENCY: CENTRAL SECURITY SERVICE (Jan. 29, 2014), http://perma.cc/6QPB-XG8H.

- Require periodic reporting by operational offices to the civil liberties office of the security contribution made by each type of surveillance authority.
- Require the Office's express comment on all proposed operational changes that sweep in more data or data for more people, particularly U.S. persons.
- Use hiring and networking to encourage Office of Civil Liberties and Privacy staff to consider civil liberties advocates as key professional reference group.
- Promote career paths for office staff that require demonstrated civil liberties expertise and commitment.

B. Civil Liberties/Privacy Official(s) in the White House

From 1999 to 2001, the Clinton Administration Office of Management and Budget had a political appointee "Chief Counselor for Privacy." Peter Swire, one of the members of the President's Review Group, served in that position, and the Review Group proposed that it be recreated, with the fancier title of "Special Assistant to the President" and the added authority that the appointee sit jointly in OMB and the National Security Council staff, and chair a Chief Privacy Officer Council "to help coordinate privacy policy throughout the Executive branch."[383] The Review Group's report explained:

> There are several reasons for creating this position: First, the OMB-run clearance process is an efficient and effective way to ensure that privacy issues are considered by policymakers. Second, a political appointee is more likely to be effective than a civil servant. Third, identifying a single, publicly named official provides a focal point for outside experts, advocacy groups, industry, foreign governments, and others to inform the policy process. Fourth, this policy development role is distinct from that of ensuring compliance by the agencies. [384]

Again, this is an Office of Goodness strategy seeking to foreground the contested values of privacy/civil liberties, this time in inter-agency processes. The President has agreed at least in part, directing designation of one or more senior "Privacy and Civil Liberties Policy Official[s]" on the National Security Council staff, the Office of Management and Budget, and

---

[383] REVIEW GROUP REPORT, *supra* note 333, at 21.

[384] *Id*. at 195. *See also* Peter Swire, *The Administration Response to the Challenges of Protecting Privacy* (Jan. 8, 2000) (unpublished manuscript), http://perma.cc/8U45-EEL2.

at the Office of Science and Technology Policy.[385] These officials were duly designated in spring 2014.[386]

The designation of White House civil liberties officials poses a risk: it seems to me that it would be nearly impossible, bureaucratically, for an agency's civil liberties officer to sustain a position even a little bit to the left of such officials on any issue with a high enough profile to receive White House attention. Perhaps this risk is not too significant, at least in a Democratic administration, when White House officials are unlikely to be to an NSA officer's right. After all, advocacy groups could complain vociferously if they deem the persons chosen unsuitable. In addition, White House officials are under less pressure to be collegial with agency staff, and also can meet more comfortably with outsiders. There is, in fact, a new committee bringing together advocacy organizations to meet with White House officials and share their views and priorities.[387] Finally, the fact that there are three such officials named might allow them to reinforce each other's commitments, even in the face of pushback by the operational agencies. So the newly designated White House staffers *may* be able to maintain civil liberties values in the policy debate at the White House, countering the ever-present pressure to focus on the more limited realm of law, compliance, and rights.

Assuming they are able to sustain both their own commitment and influence, White House civil liberties staffers can also serve as key allies to civil liberties officials within individual agencies, including the NSA. In addition, while some inter-agency councils are not terribly effective, in this situation, where part of what is needed is a secure reference group for a contested value, inter-agency councils or committees might be quite useful.[388] The point is to create a federal civil liberties bureaucracy that

---

[385] PPD-28, *supra* note 224.

[386] White House Official Interviews, *supra* note 15.

[387] The government point persons for this NGO committee are National Security Staff Senior Director Ari Schwartz and ODNI Civil Liberties and Privacy head Alex Joel. The committee is carrying out the promise made in *The Open Government Partnership, Second Open Government National Action Plan for the United States of America* 5, THE WHITE HOUSE (Dec. 5, 2013), http://perma.cc/AZL5-XYN8, in which the government committed to "Increase Transparency of Foreign Intelligence Surveillance Activities," including by "continu[ing] to engage with a broad group of stakeholders and seek input from the Privacy and Civil Liberties Oversight Board to ensure the Government appropriately protects privacy and civil liberties while simultaneously safeguarding national security."

[388] I note that, perhaps unbeknownst to the President's Working Group, there was already an interagency committee of privacy and civil liberties officials, the Privacy and Civil Liberties Subcommittee of the NSS Information Sharing and Access Interagency Policy Committee." *2013 Annual Report to the Congress: Section 5: Protecting Privacy, Civil Rights, and Civil Liberties*, INFORMATION SHARING ENVIRONMENT (2013), http://perma.cc/L94M-YTRJ ("The ISA IPC P/CL Subcommittee is comprised of senior privacy and civil liberties representatives from ISE federal mission partners as identified in EO 13358, or as designated by the Director of National Intelligence. The Subcommittee is steered by an Executive Committee of senior P/CL officers from the ODNI, DHS, and DOJ, and is

encourages its members to maintain their civil liberties commitment, including by offering some career prospects for its members with backbone. This proposal seems to me a useful piece of that strategy.

The President has not, however, committed to leaving these officials in place. Their main assignment currently is overseeing the implementation of PPD-28, which set a one-year deadline for the intelligence community agencies to issue policies implementing its new approach: "our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."[389] The three White House civil liberties officials are marching the agencies towards that deadline, in January 2015.

But the White House needs people like these, officially assigned a civil liberties role, permanently. Otherwise, as Morton Halperin, who served on the National Security Council staff from 1994-1996 explains, civil-liberties-minded staffers are apt to get shut out of national security policy development processes. Halperin explains that he was able to bring a civil liberties perspective into domestic national security policy debates on an issue or two when he was specifically asked to do so, but not more generally—his ordinary docket was foreign.[390] "The legitimacy of what you put forward is based on being able to say, well that's my role in the bureaucracy," Halperin says; "even someone [on the NSC staff] with those instincts needs that mandate to participate."[391] And at the White House, as elsewhere, Halperin says, it has sometimes been thought that "the lawyers are supposed to cover civil liberties." But, really, "they don't: they think of their job as making a legal case for what the policy people want."[392] So at the White House as elsewhere, if a civil liberties perspective is desired, the role of providing it needs to be assigned.

C. A Public Advocate in the FISA Court

Finally, it seems highly likely that in the near future, the FISA Court will gain a new process for occasional appearance of a public or special advocate. This proposal has been endorsed in varying forms by the Director of National Intelligence,[393] the President's Review Group,[394] the PCLOB,[395]

---

chaired by the ODNI Civil Liberties Protection Officer."). The committee's role has been very minimal. (Full disclosure: I chaired this committee for a period of time in 2009.)

[389] PPD-28, *supra* note 224.

[390] Halperin Interview, *supra* note 15. Halperin served on the National Security Council staff as Special Assistant to the President and Senior Director for Democracy.

[391] Halperin Interview, *supra* note 15.

[392] *Id.*

[393] *Remarks as prepared for delivery by Director of National Intelligence James R. Clapper, Open Hearing on Foreign Intelligence Surveillance Authorities, Before the S. Select Comm.*

and the President.[396] It was included in the recently-defeated Senate's USA FREEDOM Act bill, which will be one source for the next Congress's work on the issue.[397] Even former FISA presiding Judge John Bates, now the Director of the Administrative Office of the U.S. Courts, agrees in part.[398] There is, however, substantial disagreement about details—and the details matter.

The argument for such an advocate is straightforward: even if the government exhibits exemplary candor as to facts, it cannot be relied upon to brief against its own authority. Because the issues are complex and important, they deserve full adversarial development in support of better judicial decision-making. The arguments against are likewise easily summarized: There's not enough for a special advocate to do, since most issues before the FISA Court are not legally complex, and the facts will not be available to the advocate. Adversarial process will be slower and more cumbersome without leading to better decision-making. Indeed, it might lead to worse decision-making, because "adversarial process in run-of-the-mill, fact-driven cases may erode" the government's compliance with a "heightened duty of candor to the Court."[399] Indeed, "intelligence agencies may become reluctant to voluntarily provide to the Court highly sensitive information, or information detrimental to a case, because doing so would also disclose that information to a permanent bureaucratic adversary."[400]

The consensus for some form of public advocate does not encompass key details. The largest open question is about access. Under the House version of the USA Freedom Act, FISA court public advocates could have been excluded from factual or even legal presentations by the government to FISA judges and their legal advisors.[401] The Senate version of the bill, by contrast, specified that public advocates would receive "access to all relevant legal precedent, and any application, certification, petition, motion, or such other materials as are relevant to the duties of the special advocate."[402] Judge Bates, who served for six years as a FISA Court judge, has written several letters to Congress,[403] purportedly on behalf of the judiciary,[404] opposing a

---

on Intelligence, 113th Cong. (20130), (statement of James R. Clapper, Dir. of Nat'l Intelligence), http://perma.cc/Q46W-T8S4.

[394] REVIEW GROUP REPORT, *supra* note 333, recommendation 28.

[395] PCLOB, 215 REPORT, *supra* note 246, recommendation.

[396] President Barack Obama, Remarks by the President on Review of Signals Intelligence, *supra* note 326.

[397] USA FREEDOM Act of 2014, S. 2685, 113th Cong. § 401 (2013–2014); USA FREEDOM Act, H.R.3361, 113th Cong. (2013–2014), § 401.

[398] *See* sources cited *supra* note 355.

[399] Bates, *Comments on FISA Proposals*, *supra* note 355, at 7.

[400] *Id.*

[401] USA FREEDOM Act, H.R.3361, 113th Cong. (2013–2014), § 401.

[402] USA FREEDOM Act, S. 2685, 113th Cong. (2013–2014), § 401.

[403] *See* sources cited *supra* note 398.

[404] On the doubtful status of Judge Bates's claim to speak for the judicial branch, see Steve Vladeck, *Judge Bates (Unintentionally) Makes the Case for FISC Reform*, JUST SECURITY

full-time, autonomous special advocate in the FISA Court. Those letters pointed out, as a disadvantage, that inclusion of adversarial process would make the FISA Court more court-like. Judge Bates explained that "FISC judges currently have substantial flexibility in deciding how best to receive from the government information they consider relevant to a particular case." That flexibility, he suggested, could not survive *inter partes* procedural requirements:

> In order for the FISC to abide by the procedural and ethical requirements that apply in adversarial proceedings, and for the advocate to appear on equal footing with the applicant, the FISC would have to ensure that the advocate was involved in all such interactions in any case in which the advocate may participate. . . .We expect that the logistical challenges of administering such a three-way process for more than a handful of cases would be considerable.[405]

The Obama Administration, unfortunately, seems to be favoring limiting access, as well: In a letter to Senator Pat Leahy about the Senate bill, Attorney General Eric Holder and Director of National Intelligence James Clapper opined that "the appointment of an amicus in selected cases…need not interfere with…the process of ex parte [that is, one-party] consultation between the Court and the government."[406]

In fact, the FISA court and the public would be best served by a more empowered public advocate—one who is authorized to appear even without invitation from the government or the court, and, still more important, who is entitled to full access to information relevant to her duties. This would no doubt alter the current one-party procedures before the FISA court. But that's a feature, not a bug. The FISA Court's current procedures allow meetings quite unlike ordinary judicial hearings, even ex parte ones. In-advance advice from court staff to the government and iterative drafting are common. The 2009 PowerPoint slide deck already described is similarly odd for a judicial forum."[407] Other practices such as an annual lunch bringing together FISA Court judges and legal advisors (and the Chief Justice) with the heads of the CIA, NSA, and FBI likewise encourage the judges to see their own role as co-workers in the administration of the intelligence community's surveillance programs, supervising, for sure, but almost from within. If a public advocate's procedural rights disrupted this cozy relationship, that would be all to the good. The salutary effect might be to

---

(Aug. 7, 2014), http://perma.cc/BZ3A-BRUL; Letter from Chief Judge Alex Kozinski to Senator Patrick Leahy (Aug. 14, 2014), http://perma.cc/K6MY-GA6C.

[405] Bates-Leahy letter, *supra* note 355, at 6.

[406] Letter from Attorney General Eric H. Holder and Director of National Intelligence James R. Clapper to Chairman Patrick J. Leahy, Senate Committee on the Judiciary (Sept. 2, 2014), https://perma.cc/7BL6-FLTY.

[407] *See* text accompanying note 236, *supra*.

reinforce the FISA judges' role as arbiters of surveillance legality, not co-workers in the administration of the IC's surveillance programs.

If designed properly, this variation of an Office of Goodness could be essentially free from the ordinary threats to that kind of organization's influence and commitment. After all, the role of government-paid court opponent is utterly familiar from the criminal justice system. Unlike agencies, where staff must negotiate for a seat at decision-making tables, most courts have firm *inter partes* norms requiring access for all parties.[408] If Congress applies these norms to the FISA court, as it should, implementation will be very familiar. As for capture, the analogous public defenders certainly sometimes allow organizational or situational imperatives to subvert their assigned courtroom role,[409] but there seems far less reason to worry about capture in this litigation setting than inside of agencies, at least if the public advocates are not otherwise beholden to the agencies. If anything, the problem here might be too much single-minded commitment, a strict preference for civil liberties over security—but of course the court, which would remain the decider, is unlikely to become unduly single-minded. I therefore see a FISA Court public advocate as a variant on an Office of Goodness whose institutional setting would—if it is well designed—shield it from many of the landmines that usually threaten such an office's influence or commitment.

Conclusion

The development of intelligence legalism has been a major and salutary change in American governance over the past 35 years. Informed by recent unprecedented disclosures, this Article has traced the institutional arrangements that constitute the NSA's compliance ecology. Rights enunciation and compliance serve crucial rule-of-law values, and also sometimes further civil liberties. And yet they are insufficient to ensure appropriate civil liberties policy.

In his opinion for the Court last term, holding that the Fourth Amendment forbids warrantless searches of cell phones, absent exigent circumstances, Chief Justice Roberts poked some mild fun at internal

---

[408] Of course these norms may sometimes be subverted in national security cases. *See, e.g.*, United States v. Daoud, 755 F.3d 479 (7th Cir. 2014) (reversing district court order allowing defense counsel with a security clearance access to FISA information). The point is that the norms are very robust, not that they are unassailable.

[409] In his classic treatment of lawyers' sociology, Abraham Blumberg suggests that there are situations in which "[o]rganizational goals and discipline impose a set of demands and conditions of practice on the respective professions in the criminal court, to which they respond by abandoning their ideological and professional commitments to the accused client, in the service of these higher claims of the court organization." Abraham S. Blumberg, *The Practice of Law as Confidence Game: Organizational Cooptation of a Profession*, 1 L. & SOC'Y REV. 15, 19 (1967). *Cf.* Gilbert Geis, *Revisiting Blumberg's "The Practice of Law as a Confidence Game,"* 31 CRIM. JUST. ETHICS 31 (2012).

government processes as sufficient safeguards of constitutional rights. "[T]he Founders did not fight a revolution to gain the right to government agency protocols," he wrote. But he continued, and I agree, that such protocols are nonetheless "[p]robably a good idea."[410] In this post-Snowden moment, Congress can and should protect Americans' privacy and civil liberties by clamping down on bulk surveillance, creating legal rules that can then be enforced by the courts and the intelligence community's large compliance bureaucracy. But Congress and the President should not be limited by intelligence legalism. They should also follow the quite different strategy of amplifying voices *inside* the surveillance state who will give attention in internal deliberations and agency operations to civil liberties and privacy interests. But institutional design is important; civil liberties offices need deliberate and careful arrangements to safeguard their influence and commitment. If civil liberties and privacy officials inside the NSA, at the White House, and at the FISA Court can walk the tightrope of maintaining both influence and commitment, they might well make a difference—both in debates we now know about and others that remain secret. And they may help create a document trail useful for public oversight, too.

Intelligence legalism has proven unequal to the task of opposing the "collect everything" mindset. We need to add libertarian officials inside the surveillance state to nurture its civil liberties ecology. If that ecology doesn't improve, the next big leak, in five or ten or twenty years, may reveal invasions of Americans' privacy that dwarf anything we have heard about so far.

[410] Riley v. California, 134 S. Ct. 2473, 2491 (2014).