Stanford Law Review

Volume 68 May 2016

ARTICLE

The Fourth Amendment as Administrative Governance

Daphna Renan*

Abstract. Fourth Amendment law is transactional: it focuses on the one-off interaction typified by the singular investigatory search against a particular suspect for a specific crime. Yet surveillance is increasingly programmatic. It is ongoing and cumulative, and the scope of the executive's search and seizure power is determined by administrative practice. Vindicating Fourth Amendment values today requires more than what the conventional transactional approach has to offer. This Article recasts problems of surveillance as problems of governance and develops an administrative framework to help address them. Administrative law suggests a way to flesh out the requirement for Fourth Amendment "reasonableness" in the exercise of agency discretion, where today's Fourth Amendment often punts. Administrative law also provides a mechanism, independent of criminal procedure, through which courts can impose more systemic safeguards on privacy. Finally, administrative law points to a set of extrajudicial strategies for addressing surveillance at the level of governance.

* Assistant Professor, Harvard Law School. From 2009-2012, I served in the U.S. Department of Justice as counsel to the Deputy Attorney General and as an attorney-advisor in the Office of Legal Counsel. The views expressed are my own, and the discussion is based only on publicly available documents. I am grateful to Kate Andrias, Miriam Baer, Rachel Barkow, Jessica Bulman-Pozen, Adam Cox, Susan Crawford, Andrew Crespo, Ashley Deeks, Judge Harry T. Edwards, Richard Fallon, Michael Farbiarz, Jody Freeman, Barry Friedman, Trevor Gardner, Scott Hershovitz, Orin Kerr, Michael Klarman, Issa Kohler-Hausmann, Sophia Lee, Daryl Levinson, John Manning, Sandy Mayson, Gillian Metzger, Jon Michaels, Martha Minow, Saira Mohamed, Erin Murphy, Anne Joseph O'Connell, David Pozen, Natalie Ram, Dan Richman, Cristina Rodriguez, David Schleicher, Larry Schwartztol, Cathy Sharkey, Jocelyn Simonson, Jeff Singdahlsen, David Sklansky, Mila Sohoni, Carol Steiker, Matthew Stephenson, Kathy Strandburg, Cass Sunstein, Adrian Vermeule, Andrew Weissmann, Jonathan Zittrain, and to participants in workshops at the University of Chicago Law School and the University of California Berkeley School of Law for their generous engagement with this project; to Patrick Gavin, Naomi Gilens, and Connor Winn for excellent research assistance; and to the editors of the Stanford Law Review for terrific editorial assistance.

The Fourth Amendment as Administrative Governance
68 STAN L. REV. 1039 (2016)

Table of Contents

Introduction

In the Supreme Court's recent landmark decision regarding the search of a cell phone seized incident to arrest, the Chief Justice exclaimed with apparent exasperation that "[t]he Founders did not fight a revolution to gain the right to government agency protocols."[1] In holding that the Fourth Amendment requires a warrant to authorize the search,[2] the Court dug into the realities of digital data and the expansive, intrusive window that such data—which most of us carry around in our pockets—afford the government. But even as it wrestled with the implications of the digital medium, the Court clung to a conception of the search power that has long shaped Fourth Amendment jurisprudence. That conception is *transactional*: it focuses on a discrete law enforcement-citizen encounter and the question whether that one-off interaction is constitutionally reasonable.

Yet the exercise of the contemporary search power often bears little resemblance to that one-off encounter. What we have are programs of surveillance, grounded in underspecified legal mandates and implemented through an ecosystem of interacting agency protocols. Those administrative policies decide, in practice, the scope and bounds of the power to search. This may not be the Framers' vision, but it is increasingly what search and seizure looks like on the ground. Our traditional Fourth Amendment framework does not know what to do with agency protocols and the programs of surveillance they bring to life.

Recent revelations about the surveillance activities of the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) are illustrative. The NSA collects the content of hundreds of millions of communications (things such as e-mail and telephone conversations) annually under section 702 of the Foreign Intelligence Surveillance Act (FISA).[3] Extensive and interacting administrative rules from four different agencies determine the effective scope of the section 702 program. NSA rules decide, for example, whether the government can collect communications that are "about" a foreign intelligence target, rather than between that target and another individual. FBI rules decide whether the FBI can search the resulting section 702 datasets for the communications of a specific U.S. person or in the course of ordinary criminal investigatory activity.[4]

---

1. Riley v. California, 134 S. Ct. 2473, 2491 (2014).
2. *Id.* at 2485.
3. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 101, sec. 702, 122 Stat. 2436, 2438 (2008) (codified as amended at 50 U.S.C. § 1881a (2014)).
4. *See infra* notes 55-61 and accompanying text. While the agency rules developed under section 702 are reviewed by the Foreign Intelligence Surveillance Court (FISC), the

footnote continued on next page

Programmatic surveillance is not limited to the intelligence space. It is a daily feature of contemporary law enforcement. The FBI, for instance, plays a central role in linking, aggregating, and funding DNA sampling by federal, state, and local law enforcement. The FBI's database has over fifteen million DNA samples taken from convicted offenders and arrestees nationwide and used to develop investigatory leads every day across jurisdictions. Interacting agency protocols from different levels of government decide how the DNA samples will be used and searched; when information about sampled individuals will be shared; and what safeguards exist on DNA testing, sharing, retention, and use. Administrative policies decide whether law enforcement may use DNA taken from a sampled individual (such as an arrestee) to investigate that sampled individual's family members—a controversial investigatory practice known as "familial searching"—and whether any resulting lead can be shared with another law enforcement agency.[5]

While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*. Rather than responding to a single investigatory incident, the system of searches is designed en masse.[6] Surveillance is ongoing, and the implications for Fourth Amendment values such as privacy are cumulative. Technology has made it easier than ever to collect, combine, share, and retain massive amounts of data and to search the resulting datasets.[7] The parameters of these surveillance programs—what individuated searches can be run in the datasets, for what purposes, and pursuant to what limitations or protections—are designed through administrative policies.

Programmatic surveillance disrupts the legal categorizations around which our transactional Fourth Amendment law is organized. Generalized collection gives rise to individualized searches in interwoven datasets, unsettling an important distinction between individualized and suspicionless searches. Foreign intelligence gathering by the NSA, as in the section 702 program, gives rise to criminal investigatory uses by domestic law enforcement agencies, disintegrating a longstanding divide between domestic surveillance and foreign intelligence.[8] And a search of one individual implicates the privacy interests of others not subject to that initial intrusion,

---

rules governing many other surveillance activities are not. *See, e.g.*, *infra* notes 361-62 (discussing intelligence activities conducted under Executive Order 12,333).

5. *See infra* Part IV.A.2.

6. *See, e.g.*, Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159, 162 (2015).

7. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 117-21 (2008); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 318-20 (2008).

8. *See infra* Part I.B.2 (exploring these and other legal "silos" unsettled by programmatic surveillance).

such as the family members who share an arrestee's biological markers and might, in turn, be investigated through her sampled DNA.[9]

The puzzle, then, is not how to craft Fourth Amendment protections impervious to administration. It is just the opposite: How do we better integrate administrative governance with the law and theory of the Fourth Amendment? Recasting problems of surveillance as problems of governance crystallizes the limits of the traditional, transactional approach to Fourth Amendment law. A core challenge is to make administration meaningful to the Fourth Amendment. Put differently, the Fourth Amendment has stumbled upon administrative law.

A central goal of the Fourth Amendment is to curb the arbitrary exercise of the executive's search and seizure power to protect values often clustered around an idea of privacy.[10] Scholars and jurists today debate the capacity of courts and constitutional criminal procedure to achieve this goal. The idea that legislation provides a preferable alternative to robust Fourth Amendment protections is gaining traction.[11] One approach, then, might be to regard surveillance governance as a project outside of the Fourth Amendment entirely. This Article resists the trend to view legislation as an effective substitute for Fourth Amendment regulation. It argues instead for a conception of the Fourth Amendment enriched by the interaction among the branches. In this sense, my thesis is of a piece with those scholars arguing for a more "collaborative" approach to Fourth Amendment elaboration in the digital age.[12]

The Article contributes to that project by bringing sustained focus to a third cluster of institutions—the administrative state. Fourth Amendment theory tends to focus on local policing. Yet surveillance governance increasingly has a national locus as well. This is in part because of the sweeping surveillance activity in which the federal executive today engages. It is also because of the role that the federal executive increasingly plays in aggregating, linking, and funding surveillance by state and local law enforcement. The federal administrative state, then, is not simply a powerful analogy. It is an inescapable part of the story.

At a conceptual level, the Article develops this central claim: the Fourth Amendment's requirement of reasonableness in search is rarely a litmus test

---

9. *See infra* Part I.B.3.

10. *See infra* note 33 and accompanying text.

11. *See infra* Part II.B.

12. *See, e.g.*, 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, 534 (2013) (arguing that "an approach of collaborative constitutionality" between the Court and Congress "is necessary to achieve optimal levels for protecting privacy"); David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 223-24, 227-29 (2015).

applicable to an isolated incident. Instead, Fourth Amendment reasonableness should set standards for a system of governance. Constitutional reasonableness is at least in part about the interdependent processes that regularize, constrain, and make accountable the ongoing exercise of surveillance power.

The Article provides a framework to address surveillance at the level of governance. I begin with Fourth Amendment law itself and argue that the doctrines of constitutional criminal procedure can be made more attentive to how the search power is today institutionalized. Administrative law, *as an analogy*, suggests an approach to the court-agency relationship that can be integrated into constitutional reasonableness review under the Fourth Amendment. Courts also can use the core implementing device of constitutional criminal procedure—the exclusionary rule—to create incentives for more systemic extrajudicial oversight.[13]

Second, we can use administrative law *as law*. When surveillance has a national nexus, federal framework statutes like the Administrative Procedure Act (APA)—and, I will argue, FISA—supply a complementary mechanism for courts to regulate Fourth Amendment activity at the level of program design and policymaking.[14] The Fourth Amendment's primary point of entry is the warrant requirement (when it applies) on the front end and evidentiary exclusion on the back end. Yet the warrant requirement can prevent courts from meaningfully engaging with—or obscure how—front-end and back-end restrictions on surveillance practice interact or what protections are in place to safeguard the Fourth Amendment interests of individuals whose communications, biological data, or other information is indirectly acquired when surveillance activity is directed at someone else. Administrative law's framework statutes could create opportunities for doctrinal intervention different from constitutional criminal procedure and, in important respects, more amenable to the regulation of an ongoing and cumulative search power. While prevailing interpretations of the APA, to date, have stymied this development, we are seeing early signs of it in FISA and the Foreign Intelligence Surveillance Court (FISC). Yet the FISC's emergent administrative law lacks structural features that have come to legitimate administrative procedure elsewhere in the regulatory state. FISC review thus provides a

13. *See* John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CALIF. L. REV. 205 (2015) (arguing that the Supreme Court currently engages in "first-order regulation" of law enforcement by specifying what an officer must and must not do and arguing instead for a "second-order" approach where the Court instead creates incentives for political policymakers).

14. *See* Gillian E. Metzger, *The Constitutional Duty to Supervise*, 124 YALE L.J. 1836, 1843-44 (2015) (arguing that the boundary between constitutional and administrative law is increasingly "porous").

valuable window into what a more programmatic judicial role might look like but also the limitations that inhere in an emergent interinstitutional design.

Even with the help of administrative law mechanisms, however, courts are hamstrung in their ability to supervise the sprawling, interacting, and overlapping administrative policies shaping the modern power to search. Administration suggests an extrajudicial mechanism as well: policymakers can institutionalize Fourth Amendment values *through agency design*. A centralized administrative overseer, with some institutional remove from front-line actors like the NSA or the FBI, can synthesize information about the complex, interconnected policies that constitute a surveillance program and make this information more accessible and intelligible to legal and political overseers.[15] Moreover, an administrative overseer itself can engage in a more holistic, granular, and data-driven Fourth Amendment interest balancing than courts have shown a willingness to undertake.[16] In each of these ways, an administrative framework can make Fourth Amendment regulation of the search power less transactional.

The Fourth Amendment and the administrative state are no strangers. As William Stuntz memorably recounted, the origins of the Supreme Court's Fourth Amendment doctrines are rooted in federal regulatory activity.[17] According to Stuntz, the emergence of the administrative state accounts for some of Fourth Amendment law's deep pathologies.[18] Stuntz argued that a robust vision of privacy under the Fourth Amendment could not coexist with

15. *See* Matthew C. Stephenson, *Information Acquisition and Institutional Design*, 124 HARV. L. REV. 1422 (2011) (exploring how different institutional arrangements affect production of information by government actors); *see also* sources cited *infra* note 346.

16. Administrative law scholars are actively exploring how agencies implement the Constitution. *See, e.g.*, WILLIAM N. ESKRIDGE JR. & JOHN FEREJOHN, A REPUBLIC OF STATUTES: THE NEW AMERICAN CONSTITUTION (2010); Jeremy K. Kessler, *The Administrative Origins of Modern Civil Liberties Law*, 114 COLUM. L. REV. 1083 (2014); Sophia Z. Lee, *Race, Sex, and Rulemaking: Administrative Constitutionalism and the Workplace, 1960 to the Present*, 96 VA. L. REV. 799 (2010). *See generally* Gillian E. Metzger, *Administrative Constitutionalism*, 91 TEX. L. REV. 1897 (2013). For a historical discussion of the role of administrative constitutionalism in shaping Fourth Amendment doctrine, see Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 574-77 (2007), tracing the development of the Fourth Amendment idea of communications privacy to the early practice of the post office. For recent accounts in the national security context, see, for example, Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 59; and Shirin Sinnar, *Institutionalizing Rights in the National Security Executive*, 50 HARV. C.R.-C.L. L. REV. 289 (2015).

17. *See generally* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016 (1995) [hereinafter Stuntz, *Privacy's Problem*]; William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393 (1995) [hereinafter Stuntz, *Substantive Origins*].

18. *See* Stuntz, *Substantive Origins*, *supra* note 17, at 395.

the rise of the administrative state.[19] Constitutional privacy had to give out because it served as a substantive barrier to the federal government's regulation of industry—regulation that the American public had come to expect with the New Deal.[20] For Stuntz, the solution lay in seeking out other values, orienting the Fourth Amendment around the problem of police violence.[21] Police violence is surely a signal concern of the Fourth Amendment. But Stuntz was too quick to forgo the Fourth Amendment's role in regulating privacy.[22] And the rise of the administrative state itself suggests a way forward, for it has changed the legal and institutional tools available to implement constitutional values.[23] Administrative law—as an analogy for constitutional criminal procedure, as subconstitutional law, and as agency design—can help to better translate the goals of the Fourth Amendment to the realities of programmatic surveillance.[24]

---

19. *See* Stuntz, *Privacy's Problem*, *supra* note 17, at 1017-19; Stuntz, *Substantive Origins*, *supra* note 17, at 395.

20. *See* Stuntz, *Privacy's Problem*, *supra* note 17, at 1017-19; Stuntz, *Substantive Origins*, *supra* note 17, at 395.

21. *See* Stuntz, *Privacy's Problem*, *supra* note 17, at 1020, 1077.

22. The concept of privacy might itself include "a zone of personal retreat" violated by use of force or overly physically intrusive policing. *See* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1114 (2014).

23. *See* Richard H. Fallon, Jr., *The Supreme Court, 1996 Term—Foreword: Implementing the Constitution*, 111 HARV. L. REV. 54, 56-57 (1997) ("A crucial mission of the Court is to implement the Constitution successfully." (emphasis omitted)).

    In another respect, then, the administrative framework of the Fourth Amendment that I develop is itself an extension of Stuntz's work. For Stuntz widened the frame through which we study criminal justice to reveal a system of interconnected institutional players. *See, e.g.*, William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 781 (2006) (exploring the interaction between constitutional criminal procedure and the politics of crime). I take intermeshed institutional actors as a starting point and ask what types of interactions will produce an effective, integrated system of oversight.

24. The focus of this Article is the federal administrative state. Yet the project's implications are more far reaching. For local policing increasingly conducts programmatic surveillance as well, and federal, state, and local surveillance activity is often interconnected. *See* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 35 (2014); Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1325-26 (2008); Sarah Brayne, Stratified Surveillance: Policing in the Age of Big Data 3 (Mar. 30, 2016) (unpublished manuscript) (on file with author) (developing a sociological account of law enforcement-intelligence "convergence"); *see also* JOHN PODESTA ET AL., EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 49 (2014) ("Local police departments now have access to surveillance tools more powerful than those used by superpowers during the Cold War."). An administrative approach to the Fourth Amendment thus opens a broader prescriptive conversation, which I hope to elaborate in future work. For recent work proposing administrative mechanisms to enhance intergovernmental

footnote continued on next page

An earlier generation of scholars argued for local police to engage in administrative rulemaking.[25] Of this pioneering generation, Kenneth Culp Davis provided the most comprehensive argument for using administrative law to discipline police discretion.[26] Anthony Amsterdam transformed this focus on rulemaking into a theory of the Fourth Amendment, making the now-classic argument that the Fourth Amendment is a "regulatory canon" for policing.[27] The features of programmatic surveillance that I explore make these early calls for an administrative law response more urgent. Yet some of the defining problems that programmatic surveillance poses have also evolved away from this early conceptualization. Davis, for example, focused on the need for police agencies to engage in rule creation so that discretion is exercised by senior-level officials within the police department rather than the police

---

oversight of policing, see, for example, Donald A. Dripps, *Perspectives on the Fourth Amendment Forty Years Later: Toward the Realization of an Inclusive Regulatory Model*, 100 MINN. L. REV. (forthcoming May 2016); and Rachel A. Harmon, *Promoting Civil Rights Through Proactive Policing Reform*, 62 STAN. L. REV. 1 (2009).

25. *See* KENNETH CULP DAVIS, DISCRETIONARY JUSTICE: A PRELIMINARY INQUIRY 188 (1969); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 423 (1974); Carl McGowan, *Rule-Making and the Police*, 70 MICH. L. REV. 659, 690 (1972). Two scholars have sought, in recent writing, to reinvigorate the Amsterdam-Davis critique. Christopher Slobogin has embraced and built on Davis's call to use a rehabilitated nondelegation doctrine where Fourth Amendment law is unavailable to regulate surveillance. *See* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1724-25, 1758-70 (2014). While I share many of Slobogin's objectives, I have concerns about nondelegation doctrine as the vehicle for constitutional reform. *See infra* note 227. In a project contemporaneous with mine, Barry Friedman and Maria Ponomarenko argue that notice-and-comment rulemaking requirements under state administrative procedure acts should be extended to local police departments. *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1832-35 (2015). The core challenge that Friedman and Ponomarenko take up is how to extend this classic administrative law mechanism to local policing, the important project that Davis left unfinished. By developing a conceptual and analytic account of the programmatic power to search and explaining why a transactional Fourth Amendment framework fails to govern surveillance, this Article complements their effort. In contrast to Friedman and Ponomarenko, however, I situate rulemaking as one component of administrative governance and propose additional interactions between the Fourth Amendment and the federal administrative state.

26. *See, e.g.*, DAVIS, *supra* note 25; KENNETH CULP DAVIS, POLICE DISCRETION (1975) [hereinafter DAVIS, POLICE DISCRETION]; Kenneth Culp Davis, *An Approach to Legal Control of the Police*, 52 TEX. L. REV. 703 (1974) [hereinafter Davis, *Legal Control*].

27. Amsterdam, *supra* note 25, at 367. Amsterdam famously contrasted this vision of the Fourth Amendment with the then-prevailing understanding of "atomistic spheres" of individual privacy. *See id.* at 367-69. The Supreme Court has largely embraced Amsterdam's argument that the Fourth Amendment is a device to regulate policing. But the transactional framework that the Court has developed impedes those regulatory goals. *See infra* Part I.B.

officer on patrol.[28] Senior-level administrative policies today abound in the design and implementation of many surveillance programs. A core question, then, is how to create oversight institutions capable of governing these sprawling administrative policy-based regimes.[29]

At the same time, and in addition, the institutional and organizational design of federal administration has changed considerably since Davis's writing. Administrative practice is increasingly shaped by fluid program design and implementation—the work of myriad and interconnected actors.[30] Programmatic surveillance is reflective of this broader trend. The legitimacy of administration thus depends not exclusively on prior authorization but also on governance—on institutional, organizational, and doctrinal mechanisms to improve transparency; enable a more "diffuse democratic" input; provide for ongoing supervision; and, where appropriate, enable programmatic redesign.[31]

---

28. *See, e.g.*, DAVIS, POLICE DISCRETION, *supra* note 26, at 2 ("Enforcement policy is made mainly by patrolmen, who are least qualified to make it . . . .").

29. Methodologically, my project joins those working at the intersection of the fields of administrative law, criminal justice, and national security, *see, e.g.*, Rachel E. Barkow, *Administering Crime*, 52 UCLA L. REV. 715 (2005); Rachel E. Barkow, *Prosecutorial Administration: Prosecutor Bias and the Department of Justice*, 99 VA. L. REV. 271 (2013); Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. 3 (2014); Dan M. Kahan, *Is* Chevron *Relevant to Federal Criminal Law?*, 110 HARV. L. REV. 469 (1996); Gerard E. Lynch, *Our Administrative System of Criminal Justice*, 66 FORDHAM L. REV. 2117 (1998); Jon D. Michaels, *The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond*, 97 VA. L. REV. 801 (2011); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1655 (2006); Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575 (2010); Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 COLUM. L. REV. 749 (2003); Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53 (2014), and those exploring the interaction between rights and structure in governance, *see, e.g.*, Heather K. Gerken, *Second-Order Diversity*, 118 HARV. L. REV. 1099 (2005); Daryl J. Levinson, *Rights and Votes*, 121 YALE L.J. 1286 (2012); Metzger, *supra* note 14; Jide O. Nzelibe & Matthew C. Stephenson, *Complementary Constraints: Separation of Powers, Rational Voting, and Constitutional Design*, 123 HARV. L. REV. 617 (2010); Shirin Sinnar, *Protecting Rights from Within?: Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013).

30. *See* William H. Simon, *The Organizational Premises of Administrative Law*, 78 LAW & CONTEMP. PROBS., nos. 1 & 2, 2015, at 69 (rejecting "strong distinction" between program design and implementation); *see also* Daniel A. Farber & Anne Joseph O'Connell, *The Lost World of Administrative Law*, 92 TEX. L. REV. 1137, 1156-57 (2014).

31. *See* Simon, *supra* note 30, at 62 ("In postbureaucratic organization, legitimacy depends less on prior authorization than on transparency and consequent openness to ongoing diffuse democratic pressures." (emphasis omitted)); *see also* Metzger, *supra* note 14, at 1840 ("[S]ystemic features of administration—in particular, internal supervision through planning and ongoing monitoring—are increasingly the linchpin for achieving accountability of federal government programs and actions.").

A modern framework thus calls for—and is able to offer—some interventions different from those that Davis and Amsterdam envisioned.[32]

The Article unfolds as follows. Part I provides a conceptual and analytic account of programmatic surveillance and the challenges that it poses for a transactional Fourth Amendment framework. Part II argues that we cannot look to Congress alone (or to legislation instead of constitutional rights) to solve the problems of surveillance governance. It argues, instead, for an approach that integrates the Fourth Amendment with administration and administrative law. The remainder of the Article builds out that framework in three steps—from "inside" constitutional criminal procedure (Part III); using subconstitutional administrative law to complement constitutional criminal procedure (Part IV); and proposing a novel type of programmatic Fourth Amendment review by an existing administrative structure, the Privacy and Civil Liberties Oversight Board (Part V). The Article concludes by suggesting how those mechanisms might interconnect.

Before turning to the argument, let me note a caveat and offer one clarification. The caveat is that this Article does not offer a new theory of the Fourth Amendment's underlying substantive values. Often those underlying

---

32. In a forthcoming article, Andrew Crespo argues that a focus on administrative mechanisms is misguided because criminal trial courts can generate "systemic facts" to regulate policing. *See* Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. (forthcoming 2016) (on file with author). Crespo valuably illuminates some systemic information available to criminal trial courts, such as the "scripts" law enforcement officers use to establish probable cause. *See id.* (manuscript at 32-38). Yet we cannot look to courts alone either to produce the systemic facts that shape programmatic surveillance or to constrain and hold accountable the agencies that will inevitably design and implement those programs. By conceptualizing administrative law as limited to an agency's own self-regulation, *see id.* (manuscript at 13), Crespo also undervalues the potential of administrative mechanisms to create interinstitutional dynamics through which one administrative actor holds another to account, *see infra* Part V.

In proposing a more integrated Fourth Amendment administrative framework, I aim to tease out the limits of either a court-centric or an administration-centric model of Fourth Amendment oversight and to develop an interlocking approach that leverages the strengths and responds to the limitations of each set of actors. *See* NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 3-6 (1994); Edward L. Rubin, *The New Legal Process, the Synthesis of Discourse, and the Microanalysis of Institutions*, 109 HARV. L. REV. 1393, 1411-12 (1996) (arguing that "[the shared] idea that there are no purely rational decisions, ideal institutions, or optimal solutions, but only second bests" is one element of an emergent synthesis in legal scholarship, an approach "concerned with practical problems of governance . . . [and] focus[ed] on the relative effectiveness of institutions in solving these problems"). In so doing, I join a great many scholars building on the legal process tradition. *See* HENRY M. HART JR. & ALBERT M. SACKS, THE LEGAL PROCESS: BASIC PROBLEMS IN THE MAKING AND APPLICATION OF LAW 168-74, 1009-10 (1994). *See generally* William N. Eskridge, Jr. & Philip P. Frickey, *An Historical and Critical Introduction to* The Legal Process, *in* HART & SACKS, *supra*, at lx-lxii, xcii-xcvi.

goals are clustered around an idea of privacy.[33] Privacy in our technologically driven and information-dependent times might itself embrace a variety of norms.[34] The Fourth Amendment is our polity's central bulwark against an arbitrary and unbridled search and seizure power; a constitutional vision of privacy should see these threats.[35] In any event, the framework that I develop is consistent with, and arguably vital to, a variety of underlying substantive theories. I therefore use the term privacy throughout as a placeholder for the cluster of values that the Fourth Amendment serves. Finally, my claim is not that administrative mechanisms on their own are sufficient to give content to the Fourth Amendment. They emphatically are not. But each potential source of Fourth Amendment oversight is deeply flawed. Our best hope lies not in any one institution but in the dynamics and counterpressures that a system of governance can produce.

I. Governance as a Fourth Amendment Problem

The Fourth Amendment guards against the executive's unreasonable exercise of search and seizure power.[36] Implementing the Fourth Amendment has not been a static process; it is instead an evolving, contextual, and functional assessment of the types of search activity that our society will tolerate.[37] A variety of doctrinal tests have evolved over time and in response to institutional, sociological, and technological changes. The formalistic and absolutist vision of the Fourth Amendment initially articulated by the Court in

33. Others have oriented the Fourth Amendment around "security" from the state, *see, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008), "interpersonal" liberty, *see, e.g.*, Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 4 (2009), "dignity," *see, e.g.*, Josh Bowers, *Probable Cause, Constitutional Reasonableness, and the Unrecognized Point of a "Pointless Indignity,"* 66 STAN. L. REV. 987, 989 (2014); John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 660, "mutual trust," *see, e.g.*, Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1754, 1757-58 (1994), or cabining executive power, *see, e.g.*, Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

34. *See* Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH L. REV. 143, 152 (2015) ("[P]recisely because of its ambiguity, privacy is a capacious enough concept to accommodate virtually all of the values commentators have said it does not encompass.").

35. This is not to suggest that the Fourth Amendment is the *only* constitutional constraint relevant to surveillance. *See, e.g.*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

36. *See* U.S. CONST. amend. IV.

37. *See* Amsterdam, *supra* note 25, at 357-58.

the nineteenth century gave way to a more contingent conception of the Fourth Amendment to accommodate the rise of the administrative state.[38] A property-based approach transformed, in *Katz v. United States*, into a privacy-based test to extend Fourth Amendment regulation to electronic surveillance.[39] More recently, property-based notions of the Fourth Amendment have reemerged in response to changing search capabilities.[40] Each of these doctrinal moves is contested; each implicates a distinct set of tradeoffs. But together they illustrate a flexible, functional Fourth Amendment right.[41] Fourth Amendment reasonableness is not an abstract conception. It should be closely attuned to how the search power is institutionalized.

This Part provides a conceptual and analytic account of the contemporary surveillance power and the challenges that it presents for the traditional Fourth Amendment framework. I begin with a brief sketch of that traditional approach. I then develop the idea of programmatic surveillance and identify three types of problems that it poses.

A. The Transactional Fourth Amendment

Modern Fourth Amendment jurisprudence developed around a transactional conception of the police-citizen encounter that, in turn, framed the legal tests governing search and seizure.[42] Fourth Amendment law focuses on this paradigmatic question: Did the police officer have the legal authority to get his hands on the evidence?[43] Several doctrinal tests have worked to frame that judicial inquiry around the one-off interaction.

For governmental activity to come within the Fourth Amendment, it must be either a "search" or a "seizure." These are legal terms of art that trigger the Fourth Amendment's coverage. What counts as a search or seizure, under the Court's doctrines, is highly piecemeal. The traditional tests break law

38. *See generally* Stuntz, *Substantive Origins*, *supra* note 17 (discussing the evolution of Fourth Amendment doctrine away from Boyd v. United States, 116 U.S. 616 (1886)).

39. *See* 389 U.S. 347, 353 (1967).

40. *See* Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013); United States v. Jones, 132 S. Ct. 945, 949-51 (2012).

41. *See* Tracey L. Meares & Bernard E. Harcourt, *Foreword: Transparent Adjudication and Social Science Research in Constitutional Criminal Procedure*, 90 J. CRIM. L. & CRIMINOLOGY 733, 744-45 (2000) ("[R]ights [are] flexible and contextual . . . . [T]he scope of constitutional rights is more properly viewed as a vehicle to promote a vision of society rather than an inherited or cloistered stakehold.").

42. *See* Daryl J. Levinson, *Framing Transactions in Constitutional Law*, 111 YALE L.J. 1311 (2002); *see also* Mark Kelman, *Interpretive Construction in the Substantive Criminal Law*, 33 STAN. L. REV. 591 (1981).

43. *See, e.g.*, Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 828 (2010).

enforcement activity into isolated steps and ask whether each particular step, at a distinct moment in time, amounts to a search or seizure.[44]

Once the Fourth Amendment applies (that is, when a "search" or "seizure" is identified), the legal question turns to what makes the intrusion "reasonable." When the activity at issue is investigatory, the doctrine traditionally focused on the Warrant Clause.[45] The warrant provides prior authorization for a particular search in a particular place, and it creates an individuated efficacy metric: the probable cause requirement. The exercise of search and seizure power is justified under this approach—it is made "reasonable"—by that individualized showing. While the Court has recognized a variety of exceptions to the warrant requirement, these exceptions continue to understand the search as an isolated incident.[46]

The Court has increasingly turned from the warrant framework to an interest-balancing approach to reasonableness, at least when it identifies a "primary purpose" beyond ordinary crime control.[47] Though there are important differences in this approach (discussed below), the Court's frame often remains transactional in its conception of the search power.[48] Under reasonableness interest balancing, the Court asks whether the government's intrusion into the individual's constitutionally protected interest is reasonable in light of the law enforcement or governmental needs justifying the intrusion. What this often means in practice is that any programmatic consideration is one-sided: the Court will weigh law enforcement's programmatic interest in airline security or preventing drunk driving, for instance. Yet the Court generally will focus only on the immediate intrusion on privacy from the discrete search at issue.[49]

The transactional framework is further reified by the exclusionary rule, through which the Fourth Amendment is implemented in the criminal

---

44. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314 (2012).

45. On this understanding, the Fourth Amendment's Reasonableness Clause and its Warrant Clause are intertwined. *See* Amsterdam, *supra* note 25, at 395.

46. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 579 (1991) (holding that an exception to the Warrant Clause for automobile searches requires probable cause); Terry v. Ohio, 392 U.S. 1, 27 (1968) (creating reasonable suspicion standard for stop-and-frisk).

47. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000). The Court has also used this reasonableness framework in the investigatory context. *See* Samson v. California, 547 U.S. 843, 847 (2006); *see also infra* notes 98-102 (discussing Maryland v. King, 133 S. Ct. 1958 (2013)).

48. *See infra* notes 189-95 (discussing the special needs doctrine).

49. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 298 (2016) (arguing that the Court routinely compares "an apple to an orchard").

process.[50] Under the exclusionary rule, the Court determines whether the specific fruits of a particular search are admissible against a defendant. Fourth Amendment "standing" doctrine reinforces this highly individuated and one-off approach: only the person whose car is searched (not any other passenger) can challenge the search as unlawful.[51] Doctrinal limits on the availability of facial challenges further entrench the transactional framework.[52]

All of this is not to suggest that systemic judgments are absent from Fourth Amendment jurisprudence. They permeate it. But under traditional Fourth Amendment law, those systemic judgments tend to take the form of legal rules designed by courts and operating at the level of a specific police-citizen encounter. For example, the question whether a "*Terry* stop" may proceed on individualized suspicion short of probable cause constitutes a type of systemic interest balancing by judges.[53] But it is a systemic decision that imagines the search power as transactional.

B. The Inadequacy of a Transactional Fourth Amendment Jurisprudence

Contemporary surveillance increasingly bears little resemblance to that one-off encounter. Yet the idea of suspicionless searches or "dragnets" does not fully capture modern surveillance either.[54] For what begins as more generalized collection can morph into something quite different when the government runs individualized searches in its datasets. What we have are programs of surveillance, grounded in a range of legal authorities and implemented under parameters that govern collection, access, sharing, use, and

50. Exclusionary rule doctrine provides a useful opportunity to contrast what I mean by "transactional" with Amsterdam's atomistic account of the then-prevailing doctrine. The Court has explicitly embraced Amsterdam's vision of the exclusionary rule as a regulatory device for policing, rather than an atomistic personal right. *See, e.g.*, Hudson v. Michigan, 547 U.S. 586, 596 (2006). Yet the Court often continues to frame the intrusion at issue—its conception of the power to search—in transactional terms. *See id.* at 590 (focusing on the one-off refusal to comply with the knock-and-announce rule).

51. *See* Rakas v. Illinois, 439 U.S. 128, 134 (1978) (holding that an individual "aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises" lacks Fourth Amendment standing).

52. Until last Term, it was not clear whether facial challenges could still be brought under the Fourth Amendment. *See* Sibron v. New York, 392 U.S. 40, 59 (1968) ("The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case."). The Court in *City of Los Angeles v. Patel* answered this question in the affirmative, 135 S. Ct. 2443, 2449-51 (2015), but the dissent elaborated the limited utility of facial challenges in making out a Fourth Amendment claim, *id.* at 2458 (Scalia, J., dissenting).

53. *See* Meares & Harcourt, *supra* note 41, at 737.

54. *See, e.g.*, Christopher Slobogin, *Government Dragnets*, 73 LAW & CONTEMP. PROBS., Summer 2010, at 110 (defining government dragnets as group-based intrusions or deprivations of liberty, where most individuals in the group are concededly innocent).

retention. Those parameters are generally underspecified in the underlying legal authority. Elaborated at the administrative level, they can engage a web of interacting administrative actors.

Section 702 of FISA, for example, authorizes surveillance of non-U.S. persons overseas to acquire foreign intelligence.[55] As a recent report by an administrative review board explained, section 702 forms the legal basis for a

> complex surveillance *program* . . . that entails many separate decisions to monitor large numbers of individuals, resulting in the annual collection of hundreds of millions of communications of different types, obtained through a variety of methods, . . . and involving four intelligence agencies that each have their own rules governing how they may handle and use the communications that are acquired.[56]

The FBI receives raw data collected under section 702[57] and "[w]ith some frequency" queries those datasets in the service of its domestic criminal law enforcement mission.[58] The statutory authority requires the targets of section 702 collection to be non-U.S. persons believed to be overseas. So the targets are generally understood to fall outside of the Fourth Amendment's coverage under current law.[59] Yet many domestic communications and communications involving U.S. persons are also acquired.[60] Administrative rules decide in the first instance when an agency like the FBI can search the resulting datasets for a specific U.S. person and pursuant to what safeguards.[61]

As this example illustrates, programmatic surveillance is *ongoing*. I mean this in two ways. Actual collection or acquisition of information is often continuous. And, irrespective of whether acquisition is continuous, the government's uses of the data are ongoing. New searches or "queries" are regularly run in the section 702 datasets.[62] This means that the implications of programmatic surveillance for Fourth Amendment values like privacy are *cumulative*. What we have are overlapping, intermingled processes of

55. *See* 50 U.S.C. § 1881a (2014).

56. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 86 (2014) [hereinafter PCLOB SEC. 702 REPORT], https://www.pclob.gov/library/702-Report.pdf.

57. *Id.* at 34.

58. *See id.* at 58-59.

59. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990) (holding that the Fourth Amendment "has no application" to a physical search in a foreign country of the residence of a citizen of that country who has no voluntary attachment to the United States). *See generally* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 336-43 (2015) (describing and analyzing the territorial Fourth Amendment).

60. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 25-26.

61. *See id.* at 55-60.

62. *See id.*

collection, sharing, retention, and use. The resulting system of searches can impinge on new and different Fourth Amendment interests (for example, when section 702 collection sweeps up U.S. persons' communications). And the privacy incursions that this system of searches generates is not fixed but *fluid*. In fact, those incursions can become more intrusive at later phases of program implementation, such as when the section 702 datasets are searched for cumulative interactions involving a particular individual.

Modern surveillance often begins, then, with an affirmative legal authority like the section 702 statute. But that legal rule is only the seed. It will sprout a range of administrative policies that govern how information is collected, under what terms and by whom it can be accessed, when and how it can be used, for how long it can be retained, and with whom it can be shared. Other agencies will receive the data collected, and they will also develop their own rules for what they can do with the data, when, and how. This ecosystem of interdependent administrative policies is what, in practice, determines the scope of the executive's surveillance power.[63] The constitutive agency policies are developed by multiple actors, sometimes in fragmentary fashion, with varying levels of formality, visibility, and oversight. This is programmatic surveillance, and a transactional Fourth Amendment framework simply cannot govern it.

While foreign intelligence programs provide an especially salient illustration, it is a mistake to conceptualize the problem as limited to this space. Indeed, other types of surveillance programs have flourished with even fewer structural and procedural safeguards. The Drug Enforcement Administration (DEA), for instance, reportedly conducted a telephone metadata program for over two decades, collecting information on virtually all calls from the United States to as many as 116 countries with connections to drug trafficking.[64] The program, which was recently discontinued, was implemented through the use of administrative subpoenas—a legal authority designed for one-off investigatory interactions—and regulated exclusively by administrative protocols put in place, and changed over time, with no public or judicial scrutiny.[65]

Programmatic surveillance occurs at every level of government.[66] Yet the examples that follow also point to a *national* locus of power. This is in part

63. My use of the term "ecosystem" seeks to capture the idea of interdependent administrative policy-based systems. I do not mean to suggest that these interrelationships create stable equilibria.

64. *See* Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 8, 2015, 10:36 AM EDT), http://usat.ly/1FyBMkt.

65. *See id.*

66. *See, e.g.*, Brayne, *supra* note 24 (providing a sociological account of law enforcement and intelligence convergence in the age of big data).

because of the broad sweep of surveillance activity in which the federal executive today engages. It also is because of the role that the federal executive increasingly plays in aggregating, linking, and funding surveillance programs administered by state and local law enforcement. This national locus presents a set of regulatory opportunities to which I will return below.[67] My goal in this Part is to show why vindicating Fourth Amendment values in an age of programmatic surveillance requires more than what the traditional approach to Fourth Amendment law has to offer.

Programmatic surveillance poses three types of problems for a transactional Fourth Amendment framework. First, it presents a variety of *aggregation* problems obscured by Fourth Amendment law's focus on discrete interactions.[68] Second, transactional Fourth Amendment law organizes search and seizure restrictions around legal *silos*; it creates categorizations that programmatic surveillance disrupts. Third, programmatic surveillance exacerbates what we might think of as Fourth Amendment *spillovers*: search activity directed at one group will affect the Fourth Amendment interests of a different group entirely. The transactional Fourth Amendment framework often fails to see, let alone address, each of these problems.

1. Aggregation

While Fourth Amendment law focuses on the one-off interaction, surveillance is cumulative across time, space, people, and types of collection. Fourth Amendment law has developed few tools to put those pieces together, to see a whole greater than the sum of its parts.

In some ways, aggregation has posed an enduring challenge for Fourth Amendment law, though one not generally recognized in the case law. Tracey Meares has unpacked this "mismatch" between "level[s] of analysis" in the context of stop-and-frisks.[69] As Meares explains,

---

67. *See infra* Parts III-V. For exploration of the changing boundaries between federal and local policing, see, for example, Rachel E. Barkow, *Federalism and Criminal Law: What the Feds Can Learn from the States*, 109 MICH. L. REV. 519, 521 (2011); Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 816 (2012); Daniel C. Richman, *The Changing Boundaries Between Federal and Local Law Enforcement*, *in* OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, NCJ 182409, BOUNDARY CHANGES IN CRIMINAL JUSTICE ORGANIZATIONS 81 (2000); Daniel Richman, *The Past, Present, and Future of Violent Crime Federalism*, 34 CRIME & JUST. 377, 404-05 (2006); and Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289, 290-92 (2012).

68. In the legal scholarship, this is probably the most familiar of the Fourth Amendment problems posed by contemporary surveillance. Scholars have used the term in a few different ways, which I synthesize and build on below.

69. Meares, *supra* note 6, at 162.

> [W]hile the Court in *Terry* [*v. Ohio*] authorized police intervention in an individual incident when a police officer possesses less than probable cause to believe that an armed individual is involved in a crime, in reality stop-and-frisk is more typically carried out by a police force en masse as a program.[70]

This tension created a variety of doctrinal difficulties in *Floyd v. City of New York*, a challenge to the New York City Police Department's (NYPD) stop-and-frisk program.[71] A core challenge in the case was how to translate the individualized *Terry* test—whether the officer had reasonable suspicion that the individual was armed and dangerous—to the context of a massive and ongoing program disproportionately affecting persons of color in New York City.[72]

Technology, and the uses of data it enables, exacerbates this legal mismatch by creating or augmenting aggregation concerns both within any particular interaction and across interactions. The ongoing and cumulative nature of contemporary policing was on display in *United States v. Jones*.[73] *Jones* presented the question whether FBI use of a GPS tracking device on a suspect's car for a four-week period, resulting in a 2000-page dossier about the individual, was a "search" for purposes of the Fourth Amendment.[74] The government argued that there had been no Fourth Amendment activity at all. Law enforcement was simply "mak[ing] observations of matters in public view."[75] Current law does not provide the analytic tools to see how cumulative activity—twenty-eight days of tracking one's every move—can amount to a Fourth Amendment "search." As the court of appeals explained, what is revealed from "[t]he whole of one's movements" over twenty-eight days is far more than the sum of "the individual movements" alone.[76] It is a difference of kind, not degree, "for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life."[77] Rather than considering isolated

70. *Id.* (emphasis omitted).

71. *See* 959 F. Supp. 2d 540, 556 (S.D.N.Y. 2013).

72. *See id.* at 559 (noting the "inherent difficulty in making findings and conclusions regarding 4.4 million stops" because "it is impossible to *individually* analyze each of those stops").

73. 132 S. Ct. 945, 948 (2012).

74. *Id.*

75. Brief for the United States at 22, *Jones*, 132 S. Ct. 945 (No. 10-1259), 2011 WL 3561881.

76. United States v. Maynard, 615 F.3d 544, 561-62 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

77. *Id.* at 562.

bits of location data, the court of appeals recognized the cumulative effects of GPS tracking.[78]

The Supreme Court unanimously affirmed the court of appeals but splintered on the rationale for finding a Fourth Amendment search. The majority opinion, authored by Justice Scalia, decided the case on the grounds that installation of the GPS had constituted a trespass.[79] The majority opinion thus dodged the real question underlying *Jones*: When should cumulative surveillance require legal rules different from those that govern each isolated step? The separate writings in *Jones* taken together, however, suggest that a majority of the Court was troubled by the Fourth Amendment's transactional frame. Justice Alito, concurring only in the judgment and writing for four Justices, argued that the majority's trespass rationale "disregard[ed] what [was] really important" in the case—"the use of a GPS for the purpose of long-term tracking."[80] Justice Sotomayor also wrote separately to emphasize "unique attributes of GPS surveillance" that "mak[e] available at a relatively low cost . . . a substantial quantum of intimate information about any person."[81]

Jones presents the question whether a particular type of surveillance activity can amount to a Fourth Amendment search, even if isolated moments of that activity would not. Yet the context of *Jones*—a particular search against a specific suspect—obscures additional aggregation problems that programmatic surveillance poses. Consider a DEA program to collect, link, and aggregate license-plate-reader data. Police departments across the country are mounting license-plate-reader cameras on squad cars (as well as in fixed locations), so the cameras are continuously collecting time, date, and location information on vehicles in the vicinity—wherever the squad car chooses to patrol.[82] These cameras also capture detailed images of the individuals in the car and additional data.[83] The DEA, according to recently released documents,

78. This approach is what some have called an emergent "mosaic theory" of the Fourth Amendment. *See generally* Kerr, *supra* note 44 (describing and critiquing the mosaic theory).

79. *See Jones*, 132 S. Ct. at 950-54.

80. *Id.* at 961 (Alito, J., concurring in the judgment) (emphasis omitted).

81. *Id.* at 955-56 (Sotomayor, J., concurring).

82. *See, e.g.*, Letter from John Gaw, Sergeant, L.A. Cty. Sheriff's Dep't, to Jennifer Lynch, Attorney, Elec. Frontier Found. (Sept. 5, 2012), https://www.eff.org/document/la-sheriffs-dept-automated-license-plate-reader-system-information; L.A. Cty. Sheriff's Dep't, Automatic License Plate Recognition—ALPR, PowerPoint Presentation 3 (2014), https://www.eff.org/files/2014/07/16/lasd_powerpoint-boss.pdf; Craig Timberg, *License-Plate Cameras Track Millions of Americans*, WASH. POST (July 17, 2013), http://wpo.st/AudW1.

83. In Los Angeles, for example, this has amounted to data on nearly three million cars per week, which are stored for a period of years and shared with dozens of other law

footnote continued on next page

has developed a National License Plate Recognition Initiative, which aggregates and links ongoing license-plate-reader data collected by various federal, state, and local agencies.[84] The Department of Homeland Security (DHS) had similarly considered (but for the moment appears to have scrapped) its own national license plate data initiative,[85] and private license plate aggregation services are expanding in reach and in governmental clientele.[86]

If license plate data are being collected wherever law enforcement patrols, there is a genuine risk that the data overwhelmingly pertain to underprivileged communities and the communities of color where we see more policing. These datasets are themselves becoming investigatory tools for law enforcement, but they can be investigatory tools populated by the movements of particular groups. We saw this in the stop-and-frisk program in New York City, where law enforcement initially used stop-and-frisk encounters to compile a dataset of the movements of the individuals stopped. The database, intended by law enforcement to be a resource for future investigatory work, was effectively a dataset of the movements of African-American and Latino individuals in New York City.[87] The transactional Fourth Amendment framework fails to address—indeed, it cannot even see—these cumulative implications for Fourth Amendment values.[88]

---

enforcement agencies. *See* ACLU v. Superior Court, 186 Cal. Rptr. 3d 746, 749 (Ct. App.), *review granted*, 352 P.3d 882 (Cal. 2015).

84. *See* Devlin Barrett, *U.S. Spies on Millions of Drivers*, WALL ST. J. (Jan. 26, 2015), http://on.wsj.com/1BsKCyj.

85. *See* Ellen Nakashima & Josh Hicks, *Department of Homeland Security Cancels National License-Plate Tracking Plan*, WASH. POST (Feb. 19, 2014), http://wpo.st/VwdW1. The Immigration and Customs Enforcement agency, a component of DHS, had put out a solicitation for a contractor to create the database, reportedly without the approval of agency leadership in DHS. The Secretary of DHS ordered the cancellation of the plan when it came to the attention of lawmakers and privacy advocates. *See id.*

86. *See* Cyrus Farivar, *New Software Watches for License Plates, Turning You into Little Brother*, ARS TECHNICA (Dec. 5, 2015, 9:30 AM PST), http://arstechnica.com/business/2015/12/new-open-source-license-plate-reader-software-lets-you-make-your-own-hot-list.

87. The NYPD ultimately expunged, under threat of litigation, the identifying information of all individuals whose stops did not lead to criminal convictions. *See* Joseph Goldstein, *City Agrees to Expunge Names Collected in Stop-and-Frisk Program*, N.Y. TIMES (Aug. 7, 2013), http://nyti.ms/15OA27N. Data played an important role on all sides of the NYPD stop-and-frisk program. It was plaintiffs' expert's empirical analysis of paperwork used by the NYPD to document every stop-and-frisk encounter (documentation itself required as a result of earlier litigation against the NYPD's program) that proved vital to the recent class action challenge to NYPD's stop-and-frisk program. In striking down the program, *Floyd v. City of New York* relied heavily on a statistical analysis of those individualized forms. 959 F. Supp. 2d 540, 660 (2013); *see also* Meares, *supra* note 6, at 161-62.

88. Whether racially discriminatory law enforcement implicates Fourth Amendment values or only equal protection values is contested. I join those who seek to "restore

footnote continued on next page

A different type of aggregation concern arises from the cumulative use of search tools.[89] Current technologies are increasingly sophisticated in aggregating across information streams, creating a more textured, nuanced, and comprehensive portrait of daily routines and interpersonal relations.[90] For example, the National Counterterrorism Center (NCTC), a federal agency that serves as a "central and shared knowledge bank on terrorism information,"[91] pursuant to recently revised administrative guidelines, is now authorized to create mirror images of datasets created by other federal agencies where those datasets "may . . . constitute terrorism information" and to retain and use the information for up to five years.[92] The databases, created by myriad federal agencies in the service of very different policy mandates, might include, for example, financial records or the names of individuals hosting foreign students.[93] A complex web of interagency memoranda of agreement governs sharing, use, and retention of these datasets.[94]

The cumulative implications for Fourth Amendment values like privacy mean that the Fourth Amendment interests involved can change at different phases of a surveillance program. This points us to another type of problem.

2. Silos

Fourth Amendment law protects Fourth Amendment values by organizing search and seizure into legal silos. Surveillance is directed

race to a central place in the Fourth Amendment discourse." Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 808 n.183 (engaging the leading works of Tracey Maclin, *"Black and Blue Encounters"—Some Preliminary Thoughts About Fourth Amendment Seizures*, 26 VAL. U. L. REV. 243 (1991); and Sheri Lynn Johnson, *Race and the Decision to Detain a Suspect*, 93 YALE L.J. 214 (1983)); *see also* Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 333 (1998); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 838-44 (1994).

89. *See* SOLOVE, *supra* note 7, at 117-21; Slobogin, *supra* note 7, at 318-20.

90. *See, e.g.*, PODESTA ET AL., *supra* note 24, at 4-7, 28-29; *see also* Murphy, *supra* note 24, at 1376-80 ("Discrete technological restraints on liberty can accumulate and fully fetter an individual while remaining largely disaggregated for purposes of assessing their effect.").

91. *Who We Are*, NAT'L COUNTERTERRORISM CTR., https://www.nctc.gov/whoweare.html (last visited May 5, 2016).

92. *See* Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information 9 (2012) [hereinafter NCTC Guidelines].

93. *See* Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, WALL. ST. J. (Dec. 13, 2012), http://on.wsj.com/12mlCqH; *see also* Schlanger, *supra* note 29, at 29 (suggesting that as a result of the NCTC Guidelines, *supra* note 92, "[j]ust about everything any part of the federal government knows about anyone is now potentially available for five years of big-data-mining").

94. *See* NCTC Guidelines, *supra* note 92, at 8-9.

domestically or abroad. Surveillance is about evidence gathering, foreign intelligence, or some other "special need." Surveillance is conducted by the government or by private actors. Depending on which silo you are in, the Fourth Amendment is on or off. The Warrant Clause is on or off. The constitutional rules of engagement change.

With programmatic surveillance, however, the relevant legal silo can change at different phases of the program. And this has the potential to turn Fourth Amendment protections on their head. Consider the divide between individuated searches and generalized collection. Ordinarily, individuated searches require individualized suspicion such as probable cause to justify the search and, absent an available exception, require a warrant. Generalized searches do not, and one reason for this is that the broader scope of those searched is itself understood to be a type of protection against an overreaching executive. Programmatic surveillance enables the government to begin with a more generalized sweep and then to undertake individuated searches of its choosing in the resulting datasets. Yet Fourth Amendment protections, under current law, have run out before we get to these individuated intrusions.[95]

This is because of another legal silo. The conventional Fourth Amendment inquiry focuses on the authority to collect information.[96] The usual Fourth Amendment question is whether this police officer was legally authorized to get his hands on that evidence. Did he have a warrant? Did he need a warrant? What the government does with the information it has lawfully acquired was not traditionally considered a Fourth Amendment question at all. The privacy implications of surveillance programs, however, are meaningfully determined not solely by acquisition but also by use.[97] How can the information collected under these programs be accessed, used, shared, and retained—by which agencies and pursuant to what safeguards?

In our license-plate-reader program, law enforcement officials are constantly sweeping up license plate data on individuals in the areas that they patrol. But what can law enforcement *do* with that data? When can law enforcement run an individuated search in the database? How do we translate the concerns underlying *Jones*—the government's ability to compile a lengthy

95. *See, e.g.*, Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 334 (2010).

96. *See, e.g.*, Daniel Richman, *Fifteen Years of Supreme Court Criminal Procedure Work: Three Constitutional Brushes* 20 (Columbia Law Sch. Pub. Law & Legal Theory Working Paper Grp., Paper No. 14-425, 2014), http://ssrn.com/abstract=2504692 ("Fourth Amendment doctrine has always been willfully blind to use regulation. If police can properly see and take something, [the] Fourth Amendment has been read to say virtually nothing about how the state uses it down the road.").

97. *See, e.g.*, Murphy, *supra* note 43, at 833-34; *see also* SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 223-46 (2013).

dossier with intricate details about one's daily movements—to a surveillance program where cumulative information emerges from the streams of data already in the government's datasets?

The Supreme Court in some ways appeared sensitive to use-based concerns in its foray into DNA collection in *Maryland v. King*.[98] In its background description of the relevant state statute, the Court identified statutory constraints that governed the DNA collection program.[99] But the transactional framework did not provide the Court with analytic tools to integrate those considerations into its Fourth Amendment reasonableness review. Instead, the Court looked to the statutory text only to suggest a limitation on the purpose of DNA collection itself. Under the Fourth Amendment's silos, the Court needed to conclude that the "primary purpose" of DNA collection would not be "ordinary crime control" in order to approve the warrantless collection of DNA samples from arrestees.[100] And the Court relied on a contorted reading of the statutory text to support its conclusion that the government purpose at issue was something different from routine evidence gathering.[101] The real work of the statutory scheme—its imposition of constraints on how and when DNA could be collected and retained and what kinds of searches the state could run in the database—played no apparent role in the Court's reasonableness interest balancing.[102]

Another legal silo arises from the fact that the Fourth Amendment restrains only the government from collecting information, not private parties.[103] As a result, the government can obtain information that individuals surrender to private companies such as banks or phone companies, even when it could not have collected that information itself.[104] Even as the DHS retracted

98. 133 S. Ct. 1958 (2013).

99. For example, the Maryland statute prohibits familial searching. *Id.* at 1967.

100. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

101. The Court found that the statutory purpose for the warrantless DNA collection program was "identif[ication]," rather than evidence gathering or ordinary crime control. *King*, 133 S. Ct. at 1970. That conclusion was powerfully called into question by the dissent and belied by the underlying statutory text. *See id.* at 1985-87 (Scalia, J., dissenting); *see also* MD. CODE ANN., PUB. SAFETY § 2-505 (West 2016) (detailing purposes of DNA collection).

102. *See* Erin Murphy, *The Supreme Court, 2012 Term—License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161, 163-65 (2013).

103. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . .").

104. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979); *Miller*, 425 U.S. at 443. *But see* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."). There is an extensive

footnote continued on next page

its solicitation for a nationwide license-plate-reader database in response to concerns from privacy advocates, for example, some of its agents continue to access just such a databank created through a private entity.[105]

Longstanding silos also shape foreign intelligence law under the Fourth Amendment. An important silo is the inside-outside distinction: the rules governing surveillance directed inside the United States (typically requiring a warrant when the content of communications is being acquired) are different from the rules governing surveillance directed abroad.[106] Drafted in the shadow of the Fourth Amendment, section 702 of FISA authorizes the federal executive to target individuals reasonably believed to be located outside the United States to acquire foreign intelligence information without a warrant.[107] But the statute prohibits use of the section 702 authority to target U.S. persons or those inside the United States, or to reverse target—that is, to target a person outside the United States if the purpose of collection is really directed at a known person reasonably believed to be inside the United States.[108] Many domestic communications are nevertheless swept up in the section 702 collection, and agency rules permit federal intelligence and law enforcement agencies to run queries for specific U.S. persons in those resulting datasets. This brings us to a third type of problem for the transactional Fourth Amendment.

---

literature critiquing the so-called "third-party doctrine." *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (describing the common criticisms and offering a defense of the third-party doctrine).

105. *See* Ellen Nakashima, *ICE Twice Breached Privacy Policy with License-Plate Database*, WASH. POST (Oct. 29, 2014), http://wpo.st/vBeW1. Nakashima reports that about one-fifth of Immigration and Customs Enforcement's field offices, as well as officers at the DEA, IRS, FBI, and U.S. Marshals Service, have contracts with Vigilant Solution's license plate database. The database contains more than two billion plate detections and grows at a rate of over seventy million plate detections per month. *See id.*; *National Vehicle Location Service*, VIGILANT SOLUTIONS, http://vigilantsolutions.com/products/nvls (last visited May 5, 2016); *see also* Ellen Nakashima, *A Year After Firestorm, DHS Wants Access to License-Plate Tracking System*, WASH. POST (Apr. 2, 2015), http://wpo.st/cDeW1. *See generally* Jon D. Michaels, *Privatization's Pretensions*, 77 U. CHI. L. REV. 717 (2010) (arguing that agencies work around legal and political constraints on their authority through outsourcing).

106. Philip Bobbitt has described this idea as one of the defining "antinomies" of intelligence. PHILIP BOBBITT, TERROR AND CONSENT: THE WARS FOR THE TWENTY-FIRST CENTURY 296-97 (2008). The Supreme Court has never decided whether foreign intelligence collection requires a warrant, but the courts of appeals to decide the question have embraced such an exception to the warrant requirement. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 90 & nn.411-12 (collecting cases).

107. *See* 50 U.S.C. § 1881a (2014).

108. *See id.* § 1881a(b)(2), (3).

3. Spillovers

Surveillance directed at one group can sweep up the communications or data of a different group entirely. We can think about this as a "spillover" problem. The effects of surveillance are felt by others—in the form of intrusions on the Fourth Amendment interests of individuals who are not themselves the direct targets of the search.

The paradigmatic example of surveillance used to be the wiretap. The police officer gets a warrant to wiretap the suspect's phone. Other people's communications might be "incidentally" collected, for example, when they call the suspect's phone. But this was a tightly delineated and fairly manageable problem. The inherent limits on "incidental" collection in the analog world do not translate to the digital context.[109] In fact, surveillance technologies can further exacerbate the problem. One type of collection under the section 702 program, for example, included tens of thousands of domestic communications—communications outside the scope of the legal authority for collection—because it was not technologically feasible to separate out those communications from the other discrete communications that were lawfully targeted.[110]

DNA searches lead to a different kind of spillover. Difficult questions arise as to what types of searches can be run in the DNA databases. A particularly controversial type of use is "familial searches." With this investigatory technique, the government uses DNA collected from one individual to find a potential link between that individual's relatives and a crime scene.[111] Familial searching thus implicates privacy interests beyond those of the sampled individual. Yet the question courts typically consider under the transactional Fourth Amendment framework—whether collecting DNA (for example, from an arrestee) requires a warrant—does not get at the question whether law enforcement can then use that arrestee's DNA sample to investigate a potential connection between an unsolved crime and that arrestee's family members.[112]

Cybersecurity, a top priority for the executive,[113] offers another example of spillovers. A core objective of the federal executive's cybersecurity efforts is

109. *See* Daskal, *supra* note 59, at 375-76.

110. *See* Redacted, 2011 WL 10945618, at *28-29 (FISA Ct. Oct. 3, 2011).

111. *See infra* notes 258-66 and accompanying text.

112. *See* ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 189-214 (2015).

113. *See, e.g.*, *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 9 (2013) (statement of James R. Clapper, Director of National Intelligence) ("[W]hen it comes to the distinct threat areas, our statement this year leads with cyber."); *see also* JAMES R. CLAPPER, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1-4 (2016) (discussing "cyber and technology" threats); BENJAMIN WITTES & GABRIELLA

footnote continued on next page

protecting domestic information channels from foreign threats (such as foreign nations or international terrorist groups).[114] But so safeguarding communications infrastructure inescapably requires monitoring domestic communications, most of which will have nothing to do with those foreign targets. A cybersecurity program implemented by the federal executive, for example, scans all incoming and outgoing Internet traffic on the executive's unclassified computer systems for indicia of malicious computer code.[115] "EINSTEIN," as the monitoring system is called, gives the executive potential access to every communication that traverses a government employee's computer, including correspondence in personal e-mail accounts with individuals outside of government.[116]

In 2009, the Office of Legal Counsel (OLC) responded to a request from the White House Counsel to review EINSTEIN's legality under the Fourth Amendment and the federal surveillance statutes.[117] The resulting executive branch legal opinion takes a "belt and suspenders" approach to the Fourth Amendment question and, as a result, engages with layers of the current doctrine. This textured approach shows where the Fourth Amendment runs out under current law, but it also is suggestive of what a more robust role for the Fourth Amendment in regulating surveillance programs might look like.

The OLC first considered the question whether computer users would have any "reasonable expectation of privacy" in their online communications,

---

BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES 6-7, 12-13 (2015).

114. *See, e.g.*, Harrison Donnelly, *Q&A: General Keith B. Alexander*, MIL. INFO. TECH. MAG. (Dec. 17, 2010), http://www.kmimediagroup.com/military-information-technology/articles/288-military-information-technology/mit-2010-volume-14-issue-10-november/3650-qaageneral-keith-b-alexander-sp-454 (describing U.S. Cyber Command's objectives).

115. *See* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch, 33 Op. O.L.C., 2009 WL 3029765, at *2-4 (Jan. 9, 2009) [hereinafter OLC EINSTEIN Op.].

116. *See id.* at *5.

117. The OLC opinion discussed in the text is dated January 9, 2009 and signed by then-Principal Deputy Attorney General Steven G. Bradbury. *See id.* at *33. Perhaps because the opinion was issued immediately before a new President took office, the OLC was again asked to review the EINSTEIN system. An additional opinion from the then-new Acting Assistant Attorney General for the OLC effectively adopted the earlier opinion's analysis. *See* Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch, 33 Op. O.L.C., 2009 WL 3029764 (Aug. 14, 2009). These opinions review the "EINSTEIN 2" program. For an overview of how EINSTEIN 2 fits together with other aspects of the EINSTEIN system, see *EINSTEIN*, U.S. DEP'T. HOMELAND SEC. (Dec. 14, 2015), https://www.dhs.gov/einstein.

without which there would be no Fourth Amendment "search."[118] The OLC concluded that consistent use of log-on banners alerting government employees to the monitoring would remove any reasonable expectation of privacy in an employee's e-mail communications on the computer.[119] This meant that the simple act of clicking through a log-on banner when a federal employee signed into her desktop computer in the morning removed any Fourth Amendment coverage. This is a contestable conclusion, but it is not far-fetched under current doctrine.[120] The OLC went on to consider whether the Fourth Amendment would have been violated if a reasonable expectation of privacy did exist—that is, if there had been a "search" for Fourth Amendment purposes. It concluded that a warrant would not be required under the "special needs" exception. The government had a noninvestigatory purpose for the EINSTEIN program, and an individualized warrant requirement would be impracticable.[121]

This left the question whether any search was constitutionally "reasonable." What should reasonableness mean in this context? The case law is unclear and generally permissive.[122] In keeping with innovations from the FISC in the FISA context to which I return below, the OLC turned its attention to the governance tools that would safeguard privacy after the initial collection of domestic communications. These included administrative restrictions on when and with whom information derived from the program could be stored or shared and procedures designed to minimize the acquisition and use of nonpublic information about U.S. persons.[123] The OLC further emphasized the

118. After *United States v. Jones*, 132 S. Ct. 945, 949 (2012), a trespass could also give rise to a Fourth Amendment "search."

119. OLC EINSTEIN Op. at *11. The OLC also concluded that individuals in the private sector communicating with executive branch employees lacked a reasonable expectation of privacy in the content of their communications under current Fourth Amendment law because those individuals had assumed the risk that the government would monitor their communications when they chose to communicate with the government employee. *See id.*

120. The OLC's analysis relied on court of appeals decisions holding that state or federal employees (for example, at a university) lacked a reasonable expectation of privacy in their e-mail communications on work computers where computer use policies advised employees that the system would be monitored. *See id.* at *7-10 (discussing decisions in United States v. Simons, 206 F.3d 392 (4th Cir. 2000); United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002); and United States v. Thorn, 375 F.3d 679 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005)).

121. *See id.* at *18-19.

122. *See, e.g.*, Sundby, *supra* note 33, at 1800 ("The Court's present approach [to Fourth Amendment reasonableness] approximates a loose rational basis standard: if the intrusion arguably advances the government interest, the Court will not second-guess the government's judgment.").

123. OLC EINSTEIN Op. at *19.

auditing, oversight, and training procedures that would be in place for the program's implementation.[124] This collection of administrative governance tools constitutes the only meaningful constraints on the EINSTEIN program.[125] Yet these tools come into play only after the doctrinal Fourth Amendment has already run out.

Another point is worth noting given the preference that some scholars have expressed for statutory substitutes to the Fourth Amendment—a set of claims to which the Article turns below. Administrative governance (other than the log-on banners) did not factor into the question whether EINSTEIN complied with any of the four key surveillance statutes.[126]

II. The "Interlocking Gears" of Fourth Amendment and Administrative Law[127]

A. Beyond Warrants

As the foregoing shows, the transactional framework fails to expose or govern how the search power is today institutionalized. The Fourth Amendment itself describes a particular relationship. The Warrant Clause interposes a neutral arbiter at a remove from the passions of the officer in the field. This external overseer evaluates the government's desired conduct against the probable cause metric and demands particularity and reason-giving by the government prior to search. As a functional matter, these requirements constrain and hold accountable—they legitimate the exercise of surveillance power.

Yet the warrant requirement on its own is ill suited to govern programmatic surveillance. To be sure, particular facets of surveillance programs might require a warrant. And the Supreme Court has usefully

124. *Id.* at *18.

125. Technology might be understood to impose additional constraints relevant to the Fourth Amendment, for example, by limiting the types of searches that can be conducted or the types of information that can be retained. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71-73 (2013).

126. The OLC considered the EINSTEIN program under the Wiretap Act, FISA, the Stored Communications Act, and the Pen/Trap Act. Relying on judicial precedent, the OLC determined that, where log-on banners or computer-use agreements are consistently employed, the consent exception available under each of those statutory schemes would apply. OLC EINSTEIN Op. at *28.

127. *See* Heather K. Gerken, Windsor*'s Mad Genius: The Interlocking Gears of Rights and Structure*, 95 B.U. L. REV. 587, 588 (2015) (arguing that federalism and the First Amendment are "like two interlocking gears, moving the . . . constitutional project of integration forward").

extended the warrant requirement in cases like *Riley*.[128] But unless we construct a system of warrants on top of warrants to face the reality of searches on top of searches described above, the warrant framework will not mediate the various points at which surveillance programs implicate additional and distinct Fourth Amendment interests; it will not address spillovers. Requiring a warrant to obtain an arrestee's DNA sample, for example, would not address the question whether that arrestee's family members may be targeted through familial searching.

Nor is the warrant requirement an effective mechanism for addressing searches in the aggregate, for seeing the interactive effects of the parameters that shape a particular surveillance practice. It might be that programs with more permissive rules governing initial collection should be subject to more stringent access restrictions or other types of back-end privacy safeguards.[129] Finally, warrants lack a mechanism to determine whether just cause continues to support the ongoing exercise of surveillance power. The warrant is not a tool through which ongoing search activity can be revisited as societal and technological facts on the ground evolve.

In each of these respects, the limitations of the warrant framework are reinforced by the deeper transactional methodology underlying constitutional criminal procedure.[130]

---

128. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2493 (2014) (holding that search of cell phone incident to arrest requires a warrant).

129. *See, e.g.*, PCLOB SEC. 702 REPORT, *supra* note 56, at 96 ("[G]iven the comparatively low standards for *collection* of information under Section 702, standards for querying the collected data to find the communications of specific U.S. persons may need to be more rigorous than where higher standards are required at the collection stage.").

130. The inability of a transactional Fourth Amendment framework to respond to programmatic surveillance is reflective of a broader disconnect between systemic administration and constitutional law. *See* Metzger, *supra* note 14, at 1859-70 (describing standing doctrine, Eighth Amendment and due process doctrine, and the prohibition on respondeat superior liability as obstacles to a constitutional duty to supervise).

Institutional reform litigation might initially be seen as an exception to this phenomenon. Yet, as Metzger argues, courts have consistently limited the viability of institutional reform litigation as a response to systemic problems. *See id.* at 1860. This is especially true in the Fourth Amendment context. *See, e.g.*, Harmon, *supra* note 24, at 3, 11-13. To be sure, institutional reform litigation has had some important successes in subjecting program design to Fourth Amendment review. *See, e.g.*, Floyd v. City of N.Y., 959 F. Supp. 2d 540, 658, 660 (S.D.N.Y. 2013) (ruling in favor of Fourth and Fourteenth Amendment challenges to the NYPD's stop-and-frisk program). But *Floyd* itself suggests success is dependent as much on politics as law. Real questions persist as to the availability of a Fourth Amendment claim to address the programmatic harms of stop-and-frisk. *See supra* Part I.B.1. It was ultimately a mayoral campaign promise that terminated the litigation and helped realize the judicially imposed remedies. *See* Benjamin Weiser & Joseph Goldstein, *Mayor Says New York City Will Settle Suits on Stop-and-Frisk Tactics*, N.Y. TIMES (Jan. 30, 2014), http://nyti.ms/1ff11Km. For an

footnote continued on next page

B. Statutory Surrogates and the Inevitability of Delegation

Some scholars and jurists argue that surveillance should be regulated by Congress through statutes instead of by courts and the Fourth Amendment—a position that "may be approaching the status of conventional wisdom."[131] Most prominently, Orin Kerr has argued in a series of works that Congress should create legal rules to regulate emergent surveillance technologies instead of Fourth Amendment law.[132] Kerr would limit the Fourth Amendment's coverage when surveillance technologies are in flux,[133] and he would design interpretive rules that require Congress to resolve statutory ambiguity instead of courts.[134] In combination, his proposals put Congress in charge of privacy and depend on "legislative rule-creation" to protect constitutional interests.[135]

Kerr identifies important limitations on judicial capacity to confront emergent surveillance tools. His treatment of Congress, however, is incomplete. Congress rarely (if ever) designs surveillance programs holistically or with the granularity needed to achieve meaningful oversight on its own. Erin Murphy's canvassing of privacy statutes reveals that Congress legislates

---

argument that institutional reform litigation itself is an important type of "noncanonical" administrative law, see Simon, *supra* note 30, at 92-94. *See also* Harmon, *supra* note 24, at 4-7 (arguing that the U.S. Justice Department's Civil Rights Division should use "a regulatory approach [under its 42 U.S.C. § 14141 authority] rather than litigation to effectively reduce police misconduct nationwide" by adopting an enforcement strategy that "make[s] the net expected cost of reform less than the net expected cost of misconduct").

131. Sklansky, *supra* note 12, at 225, 227 (describing and critiquing this development); *see Riley*, 134 S. Ct. at 2497-98 (Alito, J., concurring in part and concurring in the judgment) ("Legislatures . . . are in a better position than we are to assess and respond to the changes [involving privacy] that have already occurred and those that almost certainly will take place in the future."); United States v. Jones, 132 S. Ct. 946, 964 (Alito, J., concurring in the judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

132. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805-06 (2004) [hereinafter Kerr, *New Technologies*]; Kerr, *supra* note 44, at 350; Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 1514-15 (2014) [hereinafter Kerr, *Rule of Lenity*]; *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 541-42 (2011). *But see* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 166-67 (2011); Murphy, *supra* note 12, at 495-96; Sklansky, *supra* note 12, at 224, 227-29. The debate over the allocation of power between courts and Congress in criminal procedure extends well beyond the surveillance context. *See, e.g.*, David Alan Sklansky, *Killer Seatbelts and Criminal Procedure*, 119 HARV. L. REV. F. 56, 59-61 (2006); Stuntz, *supra* note 23, at 791-92; Robert Weisberg, *First Causes and the Dynamics of Criminal Justice*, 119 HARV. L. REV. F. 131 (2006).

133. Kerr, *New Technologies*, *supra* note 132, at 805; *see also* Kerr, *supra* note 44, at 350.

134. *See* Kerr, *Rule of Lenity*, *supra* note 132, at 1514.

135. Kerr, *New Technologies*, *supra* note 132, at 859.

with considerably less specificity.[136] As political scientists have shown, Congress's unwillingness to prescribe detailed rules for dynamic and complex regulatory domains is in part what accounts for the creation of the administrative state.[137] Congress routinely delegates program design to agencies.[138] In the context of controversial and dynamic surveillance technologies, Congress is especially likely to leave facets of the legislative framework underspecified. These issues require considerable technical expertise.[139] Identifying specific beneficiaries of effective surveillance policy in the populace is difficult, and well-formulated policy will tend to go unnoticed, while poorly formulated policy can have cataclysmic effects. Indeed, even sound policy can be the source of blame following a significant public safety or security incident. Inevitably, then, statutes in the context of emergent surveillance technologies will delegate some amount of lawmaking away from Congress.[140]

Kerr has proposed a doctrinal response to this problem, at least in the context of national security surveillance. He argues that Congress should mandate (and courts should apply) a "rule of lenity" to prevent judicial elaboration of surveillance statutes. Specifically, Kerr argues that Congress should require courts to apply a rule of lenity to the foreign intelligence authorities contained in Title 50 of the U.S. Code. Kerr would use the rule of lenity canon to shift policymaking back to Congress when statutory ambiguity

136. *See* Murphy, *supra* note 12, at 495-96.

137. Building on earlier work in transaction cost economics, David Epstein and Sharyn O'Halloran argue that Congress is more likely to "make" policy on its own when those decisions appease identifiable constituencies (tax policy is the classic example of this) and when those decisions do not require technical expertise. Congress, however, will delegate policymaking away—it will "buy" it from another institutional actor—when specific beneficiaries are more elusive and effective policymaking depends on technical information. DAVID EPSTEIN & SHARYN O'HALLORAN, DELEGATING POWERS: A TRANSACTION COST POLITICS APPROACH TO POLICY MAKING UNDER SEPARATE POWERS 203 (1999). Similarly, Congress is more likely to delegate where effective policymaking is likely to slip under the radar but poorly formulated policy "can have disastrous effects." *Id.* at 206.

138. Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1667, 1695-96 (1975). Dan Kahan has extended this explanatory account to federal criminal law. *See* Dan M. Kahan, *Is* Chevron *Relevant to Federal Criminal Law?*, 110 HARV. L. REV. 469, 488-89 (1996).

139. *See* Kerr, *New Technologies*, *supra* note 132, at 875-76.

140. *See* Aziz Z. Huq, *Structural Constitutionalism as Counterterrorism*, 100 CALIF. L. REV. 887, 918-27 (2012) (arguing Congress lacks the incentives and the means to effectively regulate counterterrorism).

arises.[141] He argues that a rule of lenity would create greater transparency and more democratically accountable surveillance.[142]

I share Kerr's desire for greater transparency and accountability in surveillance lawmaking. I also agree with him that courts are ill equipped to comprehensively craft the legal rules governing surveillance in the first instance. But I have grave doubts about putting Congress alone in the driver's seat.[143] Congress might step in to create or prohibit a politically salient surveillance authority, as it recently did in connection to the section 215 program under FISA.[144] But Congress is not well suited to micromanage program design and implementation through statutes alone. Even if Congress did legislate at the level of specificity that would be necessary to give meaningful guidance, those policy choices would quickly become obsolete. Kerr himself emphasizes that surveillance technologies are dynamic. Congress has not shown a willingness to perpetually update statutes to adapt to technological change.[145] Even if Congress were inclined to do so in the context of surveillance, legislation is too cumbersome a tool to create detailed rules when technology is in flux.[146] Finally, Congress is simply incapable of anticipating the full range of legal questions that a program of surveillance will present over time.

The technologically complex and necessarily iterative process of giving content to Fourth Amendment protections is illustrated by the discovery of multiple-communication transactions being collected under the section 702 program. As detailed above, section 702 authorizes foreign intelligence collection of the content of Internet communications, under certain circumstances, when the target is "reasonably believed to be located outside the

---

141. Kerr, *Rule of Lenity*, *supra* note 132, at 1514-15. Kerr limits the rule of lenity proposal to foreign intelligence surveillance, but he has advanced a broader version of this argument in other work. *See* Orin S. Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire*, 102 MICH. L. REV. 933, 940 (2004) ("The combination of judicial caution in the constitutional area and judicial boldness in the statutory area might lead to an optimal solution. Courts could further Fourth Amendment values by protecting privacy through statutory construction.").

142. *See* Kerr, *Rule of Lenity*, *supra* note 132, at 1514-15.

143. *See* Murphy, *supra* note 12, at 537; Sklansky, *supra* note 12, at 228. Given the political economy of surveillance discussed in the text, it also seems unlikely that Congress would create such a rule of lenity canon for national security surveillance.

144. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015); *see also infra* note 221 and accompanying text.

145. *See, e.g.*, Jody Freeman & David B. Spence, *Old Statutes, New Problems*, 163 U. PA. L. REV. 1, 2 (2014).

146. *See, e.g.*, Adrian Vermeule, *Optimal Abuse of Power*, 109 NW. U. L. REV. 673, 683-84 (2015) ("Legislative institutions are structurally incapable of supplying policy change at the necessary rates, a point made by students of constitutional law as radically dissimilar as Chief Justice Harlan Fiske Stone and Carl Schmitt." (footnote omitted)).

United States."[147] FISA requires the executive to conduct section 702 collection pursuant to targeting and minimization procedures approved by the FISC. "Upstream collection" under section 702 requires providers who control the telecommunications "backbone" to intercept communications while they are still in transit.[148] The procedures previously submitted by the executive and approved by the FISC had authorized the NSA to acquire, through upstream collection, certain discrete communications regarding a target such as e-mails to, from, or "about" that target.[149]

But in 2011, officials in the intelligence community reportedly discovered and revealed to the FISC that any single transaction acquired as part of the NSA's upstream collection might actually include a bundle of different communications, some of which are wholly unrelated to the designated target.[150] Imagine an attempt to collect a particular e-mail about a foreign intelligence target that results in the acquisition of a bundle of communications, only one of which is about the target.[151] It simply was not technologically feasible to exclude the other (irrelevant) communications.[152]

The revelation "fundamentally alter[ed]" prior understandings about the actual scope of upstream collection.[153] Prior to this discovery in 2011, there was not even a term for the type of collection that was occurring—what the government now labeled "Multiple-Communication Transactions" (MCTs).[154] The revelation that upstream collection contained MCTs eroded two underpinnings of the FISC's prior Fourth Amendment and statutory analysis.[155] First, whereas the court had previously understood that the NSA would not acquire any communications where the sender and recipients were located inside the United States, the court now understood that separating out and preventing such acquisition was not technologically feasible. Instead, the NSA was acquiring tens of thousands of these "wholly domestic

147. 50 U.S.C. § 1881a(a) (2014).

148. *See* Redacted, 2011 WL 10945618, at *11 (FISA Ct. Oct. 3, 2011). Under a second type of section 702 collection, "PRISM collection," the government provides a "selector," like an email address, to a U.S.-based communications provider such as an Internet service provider (ISP), and the ISP gives communications to or from that selector to the government. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 7.

149. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 7.

150. Redacted, 2011 WL 10945618, at *5.

151. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 125 (distinguishing a "single, discrete communication, like a single email" from a transaction that "contain[s] a number of different individual communications").

152. Redacted, 2011 WL 10945618, at *10.

153. *Id.* at *15.

154. *Id.* at *27-28.

155. *Id.* at *32.

communications."[156] Second, while the court had previously understood that the NSA's upstream collection would only acquire communications with U.S. persons or persons inside the United States when a communication was to, from, or "about" a target, the court now understood that wholly unrelated communications with U.S. persons or those inside the United States were getting swept up in the MCTs.[157] The revised technological understanding required fundamental rethinking of the legal rules governing the program.[158]

Rather than taking the normative project of surveillance governance outside of the Fourth Amendment, a more integrated framework could leverage administration and administrative law to enable an iterative, but still legally and politically accountable, process of program design and implementation.[159] A Fourth Amendment framework more attuned to administration can achieve a more transparent and participatory surveillance lawmaking without depending on Congress alone to resolve ambiguity or plug accountability gaps at every turn. And it can preserve a constitutional foothold for courts to intervene to protect interests underrepresented in the political and administrative process.[160]

---

156. *Id.* at *33.

157. *Id.* at *35-36. The court was unable to quantify the precise effects on Fourth Amendment interests. *See id.* at *36 ("On the current record, it is difficult to assess how many MCTs acquired by NSA actually contain a communication of or concerning a United States person, or a communication to or from a person in the United States." (footnote omitted)). But it noted that the "NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream collection devices." *Id.* at *37.

158. *See* Daphna Renan, *The FISC's Stealth Administrative Law*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 121, 123-30 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016) (exploring the process that unfolded in the FISC). For an argument that "about" collection and the interception of entirely domestic communications through MCTs "pushes the NSA's actions beyond constitutional boundaries," see Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 265 (2015).

159. *See* Simon, *supra* note 30, at 69 (rejecting "strong distinction" between program design and program implementation in contemporary administration and arguing that relationship is interactive and iterative).

160. *See* United States v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938); JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 75-77, 172-73 (1980). For explorations of political process theory in the context of the Fourth Amendment and criminal procedure more generally, see, for example, Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079, 1079-81 (1993); and Christopher Slobogin, *supra* note 25, at 1745-58.

C. The Promise of a More Integrated Framework

Programmatic surveillance poses two core problems for the Fourth Amendment that are archetypal problems of administrative law. First, how do we bring the administrative actors that design and implement surveillance programs into line with a set of external values in a world of inherently underspecified legal mandates? Second, how do we make those agencies' inevitable lawmaking legitimate? These are two of the defining problems of administrative law.[161]

Under the traditional approach to the Fourth Amendment, discretion is often said to begin where the law has run out.[162] Administrative law, by contrast, embraces a set of normative commitments: to regularize, rationalize, and make accountable the exercise of administrative discretion.[163] Administrative law seeks to reconcile administrative action—including and especially policymaking in complex and controversial policy domains—with legal and political constraint; it strives to confer legitimacy on the exercise of administrative power.[164] These, of course, are goals, underrealized in administrative law itself. This is especially true as the organization of the administrative state has diverged from core understandings underlying the "canonical" administrative law doctrines.[165] Yet administrative law is more present and more nuanced than those canonical doctrines would suggest,[166]

161. *See* DANIEL R. ERNST, TOCQUEVILLE'S NIGHTMARE: THE ADMINISTRATIVE STATE EMERGES IN AMERICA, 1900-1940, at 7-8 (2014); JERRY L. MASHAW, CREATING THE ADMINISTRATIVE CONSTITUTION: THE LOST ONE HUNDRED YEARS OF AMERICAN ADMINISTRATIVE LAW 8 (2012).

162. *See, e.g.*, Bowers, *supra* note 33, at 992 (suggesting that criminal procedure doctrine "just move[s] sovereign choice indoors—into a defined legal box," but "[w]ithin that box, the arresting officer remains almost free to pick and choose between probabilistic offenders and conventional enforcement means").

163. *See* David J. Barron & Todd D. Rakoff, *In Defense of Big Waiver*, 113 COLUM. L. REV. 265, 266-67 (2013). Jerry Mashaw describes "the accountability system for administrative officials" as "span[ning] three domains"—political accountability to elected officials, legal accountability, and administrative accountability. MASHAW, *supra* note 161, at 8.

164. *See, e.g.*, Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 COLUM. L. REV. 515, 532 (2015) ("Administrative law, at root, is the process by which otherwise-unencumbered agency officials are legally and politically constrained in an effort to prevent abuse and to confer legitimacy on the power that is exercised.").

165. *See* Simon, *supra* note 30, at 61-63 (labeling doctrines of judicial review of agency rulemaking and adjudication as "'canonical' administrative law" and describing the limited ability of those doctrines to effectuate judicial control over contemporary administration).

166. *See id.*

and scholars and practitioners alike continue to refine both the goals of transparency and legitimacy and the mechanisms available to achieve them.[167]

Administration and administrative law can interact with the Fourth Amendment in a few different ways. I explain three potential relationships briefly here and then proceed to develop each in turn. First, administrative law has developed a conception of the court-agency relationship that can be integrated into doctrines of constitutional criminal procedure. Rather than designing every legal rule in the first instance, courts can supervise surveillance program design and implementation by agencies. And courts can use information generated by agencies to facilitate a more programmatic review of constitutional reasonableness under the Fourth Amendment. Courts can also use constitutional criminal procedure's core remedy to incentivize more systemic oversight by other actors. In these ways, administrative law *as an analogy* can help courts make the doctrines of constitutional criminal procedure more attentive to administration and more responsive to the challenges posed by programmatic surveillance.

Second, administrative law *as law* provides courts with a mechanism independent from constitutional criminal procedure to govern surveillance as institutionalized policymaking. Subconstitutional doctrines of administrative law, rooted in framework legislation like the APA or FISA, could offer a different point of entry for courts into surveillance governance. While recent amendments to FISA have taken some important steps in this direction, the FISC continues to operate around a warrant framework that impedes the development of a more resilient administrative Fourth Amendment law. Reimagining the FISC as an administrative law court brings into view important questions about that interinstitutional design.

Ultimately, however, judicial review itself is limited as a mechanism to govern programmatic surveillance. At its core, Fourth Amendment reasonableness is about interest balancing. It is about ensuring that governmental intrusions into privacy are justified both at inception and over time. An administrative overseer can engage in a type of Fourth Amendment interest balancing that is more holistic, more granular, and more grounded in data than the interest balancing that courts considering Fourth Amendment reasonableness have been willing to undertake. This is in part because a centralized administrative overseer is uniquely able to obtain and synthesize a range of technologically complex and rapidly changing information, from different types of administrative actors (such as lawyers, policymakers, and

167. *See* Farber & O'Connell, *supra* note 30, at 1180 (proposing reforms "to help reduce the gap between [administrative law] theory and practice"); Metzger, *supra* note 14, at 1840 (arguing that supervision is "increasingly the linchpin for achieving accountability"); Simon, *supra* note 30, at 64 (arguing for conception of "democratic legitimacy in terms of oversight" rather than prior authorization).

technologists) at different agencies, about overlapping and interacting administrative authorities and constraints.[168] Administrative oversight, then, can be more iterative and interactive than judicial review, more steeped in both organizational practice and operational facts, and more adaptive to technological change.

A grave risk with any use of administrative mechanisms in governance is runaway agencies distorting legal authorities or otherwise circumventing the democratic process. This is an enduring problem for the administrative state. It might be especially acute in the context of the Fourth Amendment, for search and seizure law constructs vital bulwarks in a world of ever-increasing surveillance capacity.[169] Agencies—and therefore administrative overseers—are also more dependent than courts on political benefactors.[170] An agency's on-the-ground abilities turn in large part on politically contingent budgets,[171] leadership appointments,[172] and relational institutional power.[173] This might mean that an agency will be more responsive to political pressures or more attentive to political constraints than a court, and it certainly means that an agency's effective power can be significantly undermined by Congress, a sitting President, or agency heads.[174] The same circumstances that make an administrative overseer more attuned to institutional and organizational practice may also make it more difficult for an administrative overseer to exercise independent judgment, especially on high-stakes security questions. There are design-related responses that can diminish, though they certainly do not eliminate, these concerns.[175]

---

168. *See, e.g.*, Cass R. Sunstein, *The Most Knowledgeable Branch*, 164 U. PA. L. REV. (forthcoming August 2016) (manuscript at 1-5, 11-12), http://ssrn.com/abstract=2630726.

169. Some scholars have suggested that distrust of executive power is a Fourth Amendment "first principle." *See* Ku, *supra* note 33, at 1326; Carol S. Steiker, *"First Principles" of Constitutional Criminal Procedure: A Mistake?*, 112 HARV. L. REV. 680, 686 (1999) (book review) (discussing and building on earlier works of Telford Taylor and Tracey Maclin).

170. *See, e.g.*, Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245, 2246-48 (2001).

171. *See, e.g.*, Rachel E. Barkow, *Insulating Agencies: Avoiding Capture Through Institutional Design*, 89 TEX. L. REV. 15, 42-45 (2010) (discussing the roles of financial resource allocation and budgeting in agency design and agency decisionmaking).

172. *See, e.g.*, Anne Joseph O'Connell, *Vacant Offices: Delays in Staffing Top Agency Positions*, 82 S. CAL. L. REV. 913, 920-21 (2009).

173. *See, e.g.*, Eric Lichtblau, *Tighter Lid on Records Threatens to Weaken Government Watchdogs*, N.Y. TIMES (Nov. 27, 2015), http://nyti.ms/1jncxLc.

174. *See id.*

175. *See, e.g.*, Barkow, *supra* note 171, at 17; Schlanger, *supra* note 29, at 54-56; Sinnar, *supra* note 16, at 1082.

Administrative implementation of the Fourth Amendment, therefore, should not displace judicial oversight. A realistic approach to surveillance governance must be layered and interactive. In what follows, I offer an initial sketch of what this more integrated framework might look like in three steps, using administrative law as an analogy, as law, and as agency design. Each approach on its own offers only a partial response to the challenges that programmatic surveillance poses for the Fourth Amendment. Administrative law-as-analogy, for example, can only offer doctrinal moves to bolster constitutional reasonableness when the activity in question is found to constitute a Fourth Amendment "search." Administrative law-as-law can enable courts to skirt the difficult question of pinpointing precisely when cumulative surveillance activity amounts to a Fourth Amendment "search," but it requires framework legislation that provides a basis for subconstitutional review by a court. And an agency overseer, in addition to the limitations detailed above, depends on courts or political overseers to provide meaningful baselines against which the agency should evaluate surveillance practice. Our potential institutional checks are flawed, incomplete, and interdependent; we make the most of them by using them in combination.[176]

III. Administration "Inside" Constitutional Criminal Procedure

This Part explores how constitutional criminal procedure can better leverage administration to respond to programmatic surveillance. Part III.A argues that courts should use constitutional reasonableness review to supervise programmatic safeguards designed in the first instance by the agencies. Part III.B shows how courts can calibrate their use of constitutional remedies to incentivize and superintend extrajudicial mechanisms for more systemic accountability and constraint.

A. Administrative Law as an Analogy for Fourth Amendment Law

Administrative law suggests a different conception of agency discretion and judicial deference to be integrated into constitutional criminal procedure. Consider the *Chevron-Mead* framework of administrative law. Under *Chevron*, the agency's choice among reasonable policies, consistent with the statutory

176. This, of course, is a central insight of separation of powers theory. And it has been extended and translated to the institutional and administrative levels. *See, e.g.*, William N. Eskridge Jr., *Expanding* Chevron*'s Domain: A Comparative Institutional Analysis of the Relative Competence of Courts and Agencies to Interpret Statutes*, 2013 WIS. L. REV. 411, 428-29; Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006); Gillian E. Metzger, *The Interdependent Relationship Between Internal and External Separation of Powers*, 59 EMORY L.J. 423 (2009); Rubin, *supra* note 25, at 1397-98, 1412.

scheme, prevails even if the court would have made a different decision in the first instance.[177] In *United States v. Mead Corp.*, the Court held that *Chevron* deference applies only where the agency acts with the "force of law" in construing a statute that it is charged with administering.[178] As a practical matter, when an agency acts with the force of law, two things are likely to happen. Power inside the agency will tend to be allocated *up*—that is, to more senior-level officials.[179] *Mead* also will allocate power *out* by creating participatory opportunities. This is because acting with legal force under the APA often (though not always) will mean acting pursuant to notice-and-comment rulemaking.[180] Whether deliberately or incidentally, then, *Mead* creates a mechanism for courts to use other actors as their more expert proxies on the front end of agency policymaking.[181] Courts create opportunities for their proxies to influence agency decisionmaking ex ante by rewarding participatory decisionmaking with greater deference ex post. Rather than simply substituting the agency's judgment for that of the court, *Mead* enhances administrative governance by calibrating judicial deference to a more accountable administrative process.

This approach to deference in administrative law—as a judicial tool for enhancing governance by agencies—can provide a useful analogy for Fourth Amendment law. In contrast to scholars who argue that deference should limit

177. *See* Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 845 (1984).

178. 533 U.S. 218, 226-27 (2001) ("We hold that administrative implementation of a particular statutory provision qualifies for *Chevron* deference when it appears that Congress delegated authority to the agency generally to make rules carrying the force of law, and that the agency interpretation claiming deference was promulgated in the exercise of that authority.").

179. *See* David J. Barron & Elena Kagan, *Chevron's Nondelegation Doctrine*, 2001 SUP. CT. REV. 201, 237; Elizabeth Magill & Adrian Vermeule, *Allocating Power Within Agencies*, 120 YALE L.J. 1032, 1061-63 (2011).

180. Notice-and-comment rulemaking is not a requirement for *Chevron* deference under *Mead*. *See Mead*, 533 U.S. at 227 ("Delegation of [the authority to act with the 'force of law'] may be shown in a variety of ways, as by an agency's power to engage in . . . notice-and-comment rulemaking, or by some other indication of a comparable congressional intent."); *see also* Barnhart v. Walton, 535 U.S. 212, 221 (2002) ("[T]he fact that the Agency previously reached its interpretation through means less formal than 'notice and comment' rulemaking does not automatically deprive that interpretation of the judicial deference otherwise its due." (citation omitted)). But agencies often resort to it because notice-and-comment rulemaking is a reliable marker of the type of agency action to which *Chevron* applies.

181. *See* Stephenson, *supra* note 15, at 1446-47, 1453 (indicating that agency overseers, such as courts, can discourage or encourage agencies to pursue certain avenues of research through burdens of proof or by refusing to consider certain types of evidence); *see also* Catherine M. Sharkey, *Federalism Accountability: "Agency-Forcing" Measures*, 58 DUKE L.J. 2125 (2009) (arguing that courts can better use information-forcing tools of administrative process to enhance their own preemption determinations).

the scope of the Fourth Amendment,[182] administrative law suggests a way to embrace a more expansive Fourth Amendment right but to reshape the court's interaction with extrajudicial overseers.[183] Administrative law, first, suggests a space for congressional authorization and policy innovation and interstitial elaboration by agencies, but within substantive legal boundaries policed by courts. Administrative law, second, shows how courts can exercise different types of doctrinal oversight, policing both the content of constitutional reasonableness at the boundaries and the processes of reasonableness inside that zone. Finally, administrative law suggests limits to the types of surveillance lawmaking that agencies should be permitted to undertake absent congressional specification.

Jurists, scholars, and an engaged public will debate the right answer at each of these steps. Indeed, each is a source of ongoing and lively debate in administrative law itself. But administrative law-as-analogy helps to identify and disentangle relevant questions and considerations for Fourth Amendment reasonableness review, and it offers building blocks for a more integrated approach to search and seizure regulation from "inside" constitutional criminal procedure.

1. Structural and systemic dimensions of reasonableness

There currently are two crosscurrents in Fourth Amendment law. On one account, the content of the Fourth Amendment right is independent of statutory and administrative mooring. The approach is reflected, for example, in the Court's opinion in *City of Ontario v. Quon*.[184] Quon was a police officer who argued that his supervisors' review of his private text messages on a police department beeper violated the Fourth Amendment.[185] One of his constitutional arguments was that the police department's search of his beeper could not be "reasonable" under the Fourth Amendment because it violated the Stored Communications Act.[186] The Court dismissed this argument

182. *See, e.g.*, Kerr, *New Technologies*, *supra* note 132, at 805-06.

183. *See* Eric Berger, *Individual Rights, Judicial Deference, and Administrative Law Norms in Constitutional Decision Making*, 91 B.U. L. REV. 2029, 2035 (2011) ("[C]ourts considering constitutional challenges to agency action should not defer reflexively without inquiring more carefully into the administrative framework within which the agency has operated."); *cf.* Samuel Issacharoff & Richard H. Pildes, *Between Civil Libertarianism and Executive Unilateralism: An Institutional Process Approach to Rights During Wartime*, 5 THEORETICAL INQUIRIES L. 1, 5 (2004) (arguing that in "extreme security contexts," courts use "a process-based, institutionally-oriented" framework to shift responsibility toward joint action by political branches).

184. 560 U.S. 746 (2010).

185. *Id.* at 750.

186. *See id.* at 764.

summarily. An otherwise reasonable search could not be rendered unreasonable under the Fourth Amendment, the Court explained, through violation of a statutory safeguard.[187] *Quon* follows in a long line of cases rejecting the idea that a violation of statute or agency protocol can undermine or cut against a finding of Fourth Amendment reasonableness.[188] Reasonableness, on this view, lacks a structural dimension; it is an exercise of judicial interest balancing devoid of interbranch considerations.

A different approach to Fourth Amendment reasonableness emerges from what today's doctrine has labeled "special needs" cases. In earlier iterations of the doctrine, the Court closely scrutinized the availability of statutory and administrative constraints.[189] In *Donovan v. Dewey*, for instance, the Court considered a constitutional challenge to a regulatory scheme authorizing the Labor Department to conduct warrantless inspections of mines under the Federal Mine Safety and Health Act.[190] The Court determined that "the statute's inspection program, in terms of the certainty and regularity of its application, provides a constitutionally adequate substitute for a warrant."[191] The Court's analysis was not limited only to the statutory requirements but also to their elaboration through federal regulation. The Court emphasized that the legislation required the Secretary of Labor to develop the statutory standards with notice to mine operators.[192] In *Dewey*, then, the content of the constitutional right was intertwined with the statutory and administrative structure. The Fourth Amendment right helped ensure that extrajudicial constraints—in the form of administrative procedure—were in place to cabin, regularize, and legitimate the exercise of discretion.[193] The Court's cases governing roadblocks have similarly identified administrative guidelines as a

187. *See id.* This bifurcation of constitutional and administrative rules also manifests in administrative law doctrines. *See* Gillian E. Metzger, *Ordinary Administrative Law as Constitutional Common Law*, 110 COLUM. L. REV. 479 (2010) (describing and critiquing the separation).

188. *See, e.g.*, Virginia v. Moore, 553 U.S. 164, 168-69, 171 (2008); California v. Greenwood, 486 U.S. 35, 43 (1988); Oliver v. United States, 466 U.S. 170, 183-84 (1984).

189. *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 269-70 (2011) (exploring the role of positive law in earlier iterations of administrative search doctrine).

190. 452 U.S. 594, 596 (1981).

191. *Id.* at 603; *see also* New York v. Burger, 482 U.S. 691, 711 (1987) (holding that a statute closely regulating the vehicle dismantling industry provided a "constitutionally adequate substitute for a warrant" (quoting *Dewey*, 452 U.S. at 603)); United States v. Biswell, 406 U.S. 311, 315 (1972) (allowing administrative searches without a warrant if those searches were limited in "time, place, and scope").

192. *See Dewey*, 452 U.S. at 604.

193. *Cf.* ERNST, *supra* note 161, at 7-8 ("[T]he reformers [of the early twentieth century] . . . designed the principles of individual rights . . . into the administrative state [through administrative procedure].").

source of constraint relevant to Fourth Amendment reasonableness.[194] As others have shown, however, the role of statutory and administrative constraints even in this sliver of doctrine has become more haphazard. The Court only occasionally recognizes statutory or administrative safeguards as relevant to reasonableness interest balancing under the Fourth Amendment.[195]

Moreover, the Court's framework is designed around a legal silo: there are investigatory searches and there are regulatory searches, and they require distinct forms of judicial oversight.[196] Investigatory searches generally require individualized suspicion and (depending on context) a warrant. The reasonableness of a "regulatory" search might turn on administrative constraints.[197] What legal box one is in turns, according to the Court, on the "primary purpose" of the government's conduct—is it evidence gathering or some kind of "special need"? As Part I demonstrated, this approach fails to govern programmatic surveillance.

The Court should recognize a claim of *programmatic* unreasonableness under the Fourth Amendment, available in *both* investigatory and special needs searches. The question for a court under programmatic reasonableness review is not whether any particular encounter requires a warrant, but whether structures and processes are in place to adequately protect Fourth Amendment interests in the aggregate, over time, and in response to spillovers. Programmatic reasonableness would not focus exclusively or even primarily on the court's own balancing of privacy intrusions and governmental needs. The question is also whether and pursuant to what protections such a balance has been struck by the political branches.[198] Fourth Amendment reasonableness, on this view, is realized through interacting safeguards—a system that involves the coordinate branches.

If Fourth Amendment reasonableness has this structural and more systemic dimension—if reasonableness is in part about the institutional dynamics through which surveillance is authorized, conducted, and

194. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 453 (1990); United States v. Martinez-Fuerte, 428 U.S. 543, 559, 560 n.14 (1976). The Court has also upheld the use of administrative process in the context of inventory searches. *See* Florida v. Wells, 495 U.S. 1, 4 (1990) (holding that an inventory search is unreasonable if no policy defines the routine steps of such a search).

195. *See* Primus, *supra* note 189, at 256, 272.

196. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 286-87 (2016) (arguing that there are "two types of searches"—investigative or regulatory—and that each requires different protections against arbitrary police discretion).

197. *See id.*

198. *See* ACLU v. Clapper, 785 F.3d 787, 825 (2d Cir. 2015) ("Ideally, [the constitutionality of a surveillance program] should be resolved by the courts . . . with due respect for any conclusions reached by the coordinate branches of government.").

superintended—then administration cannot fall outside of the Fourth Amendment. The Court in cases like *Quon* is wrong to decouple the question of Fourth Amendment reasonableness from the question whether the search at issue is ultra vires.

2. Deference as a governance tool

Administrative law suggests a way to conceptualize substantive Fourth Amendment boundaries policed by courts, with an interior zone of policy discretion subject to a different type of judicial scrutiny. The familiar *Chevron* doctrine in administrative law prescribes two types of inquiries—the first requires an independent judicial judgment about what the law prohibits or requires; the second requires the court instead to supervise agency decisionmaking.[199] We might think of Fourth Amendment reasonableness review involving both types of inquiries.

At the boundaries, courts would still exercise a substantive check on search and seizure activity. A court might determine, for instance, that prolonged GPS tracking or the search of a cell phone incident to arrest requires a warrant to be constitutionally reasonable. A court might also determine, at the margins, that a particular type of search and seizure activity is simply impermissible because it is unreasonable under the Fourth Amendment.[200] As a descriptive and normative matter, however, such judicially imposed boundaries on reasonableness are likely to remain relatively infrequent.[201]

---

199. *See* Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984); Kenneth A. Bamberger & Peter L. Strauss, Chevron*'s Two Steps*, 95 VA. L. REV. 611, 611 (2009) ("[*Chevron*'s] familiar two-step analysis is best understood as a framework for allocating interpretive authority in the administrative state; it separates questions of statutory implementation assigned to independent judicial judgment (Step One) from questions regarding which the courts' role is limited to oversight of agency decisionmaking (Step Two)."). There is a debate in the administrative law scholarship about whether *Chevron* itself is properly conceptualized as having one or two steps. *Compare* Matthew C. Stephenson & Adrian Vermeule, Chevron *Has Only One Step*, 95 VA. L. REV. 597 (2009), *with* Bamberger & Strauss, *supra* (responding to Stephenson & Vermeule with a defense of *Chevron*'s two steps). There is further confusion and inconsistent views as to what type of review *Chevron*'s "Step Two" actually entails. But the more general idea that administrative law requires courts to exercise these two types of roles—one an exercise of independent interpretive judgment and the other an oversight role—is fairly entrenched in the law and legal theory. *See, e.g.*, Peter L. Strauss, *"Deference" Is Too Confusing—Let's Call Them "*Chevron *Space" and "*Skidmore *Weight,"* 112 COLUM. L. REV. 1143, 1145 (2012).

200. These types of questions constitute what we might consider "first-order" regulation of law enforcement using constitutional reasonableness. *See* Rappaport, *supra* note 13, at 215-16.

201. *See, e.g.*, Murphy, *supra* note 12, at 544.

"*Chevron* space"[202] could enable courts to supervise surveillance lawmaking even within the zone of substantive reasonableness. And it could enable a type of review more sensitive to the structural and systemic dimensions of a surveillance program. A court could first consider whether Congress has expressly authorized or prescribed the surveillance policy at issue.[203] In the absence of legislative specificity, a court would turn to the reasonableness of the agency's own program design: Has the executive engaged in a deliberate and transparent process to conclude that the privacy intrusions are warranted?[204] Are there participatory opportunities in place to identify the relevant tradeoffs, and are administrative mechanisms in place to safeguard privacy in an iterative and ongoing fashion?[205]

Recent developments concerning "StingRays" show how administrative oversight might play into Fourth Amendment reasonableness review. StingRays, or cell-site simulators, simulate a cell tower and, as a result, direct signals from cell phones in the vicinity to the StingRay.[206] StingRays provide a valuable investigatory tool for law enforcement. Imagine a drug trafficking investigation against a target who regularly discards his cell phone and obtains a new one.[207] The StingRay can make it possible for law enforcement to identify the target's new phone number.[208] By using a StingRay in several locations where the target is known to be, law enforcement can collect information from all of the cell phones in the vicinity and use process of

202. Strauss, *supra* note 199, at 1145 ("'*Chevron* space' denotes the area within which an administrative agency has been statutorily empowered to act in a manner that creates legal obligations or constraints—that is, its delegated or allocated authority.").

203. *See* Murphy, *supra* note 12, at 540; Peter P. Swire & Erin E. Murphy, *How to Address "Standardless Discretion" After* Jones 2 (Ohio State Univ. Moritz Coll. of Law, Working Paper Series No. 177, 2012), http://ssrn.com/abstract=2122941.

204. In Part V below, I detail what such a process might look like.

205. *Cf.* David Alan Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1799-1803 (2005) (emphasizing significance of institutional structure in "reconciling police with democracy").

206. "StingRay" is the common name for a cell-site simulator device manufactured by Harris Corporation. *See* Matt Richtel, *A Police Gadget That Tracks Phones?: Shhh! It's Secret*, N.Y. TIMES (Mar. 15, 2015), http://nyti.ms/1AtkPUI. For background on the StingRay device and a discussion of the Fourth Amendment questions that it raises, see, for example, Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FEDERALIST SOC'Y REV. 1 (2016); and Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1 (2014).

207. *See In re* Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, slip op. at 1-2 (N.D. Ill. Nov. 9, 2015), http://cases.justia.com/federal/district-courts/illinois/ilndce/3:2015mc00021/317964/1/0.pdf?ts=1447161923.

208. *See id.* at 5-6.

elimination to identify the target's cell phone (the cell phone in each of the locations where the StingRay was deployed).[209]

StingRays, however, present a spillover problem. The StingRay collects not just the target's cell phone information but also the cell phone information of others in the vicinity.[210] The traditional question posed by the Fourth Amendment is whether law enforcement needs a warrant to use a StingRay. But resolving that question does not respond to spillovers—the many nontarget data acquired using the device.

Until very recently, StingRays were governed by secret protocols and used pursuant to nondisclosure agreements that largely prevented both legal and political accountability.[211] The U.S. Department of Justice (DOJ) recently adopted a public policy governing the use of StingRays.[212] The policy requires law enforcement to obtain a warrant for use of a StingRay device, unless a warrant exception (like exigent circumstances) applies.[213] But the policy also includes a number of measures designed to address spillovers. It requires, for example, that when the device is used to identify an unknown cell phone, all data collected by the StingRay must be deleted as soon as the target cell phone is identified and no less than once every thirty days.[214] The policy further requires an auditing program to ensure compliance with these rules.[215]

The DOJ policy, both at the level of rules and at the level of institutional oversight inside the agency, should have bearing on Fourth Amendment reasonableness. Use of StingRay devices without protections for those whose data are indirectly acquired should be programmatically unreasonable under the Fourth Amendment. Where a policy is adopted by agency leadership and made public, however, it makes sense for a court to defer to the DOJ's choice among reasonable safeguards (for example, the frequency of data deletion or the nature of oversight inside the agency).

Some magistrate judges, recognizing the programmatic dimensions of contemporary surveillance discussed above, have started to impose their own regulatory requirements on certain types of collection—what we are seeing, in effect, is rulemaking by magistrate judge. One magistrate judge reviewing the government's use of StingRays, for instance, recently adopted a set of measures designed to protect "innocent third parties[]" whose data would be

209. *See id.* at 6.

210. *See id.* at 7.

211. *See id.* at 2, 4.

212. U.S. Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (2015), http://www.justice.gov/opa/file/767321/download.

213. *Id.* at 3-4.

214. *Id.* at 6.

215. *Id.*

inadvertently acquired.[216] Rulemaking by magistrate judge raises difficult doctrinal and normative questions under the Fourth Amendment.[217] Fourth Amendment reasonableness review that requires agencies to put administrative procedures in place to govern the use of a StingRay avoids the legal and policy concerns with rulemaking by magistrate judge, while incentivizing and creating an opportunity for courts to review rulemaking by agencies. Importantly, this type of programmatic reasonableness review enables courts to consider systemic oversight beyond rulemaking (such as audits, supervisor signoffs, and other forms of ongoing monitoring that the agency has put in place).

3. Limits to judicial deference under the Fourth Amendment

Administrative law points to a related set of questions, however: Are there limits to the types of legal rules that can be left to the agency itself to design? Myriad consequential rules for surveillance programs will inevitably be made in the first instance by agencies. Are there some types of programmatic decisions that an agency simply should not be permitted to make under the Fourth Amendment—at least absent explicit congressional specification? In the administrative law context, the Court has held that *Chevron* does not apply to a legal question of such "deep 'economic and political significance'" as to be "central" to the underlying statutory design.[218] *King v. Burwell*, the Court's recent decision on the Affordable Care Act, reinforced the idea that some legal questions are so significant that a court must undertake to resolve them independently—that is, that the legal question is not a candidate for "*Chevron* space."[219]

---

216. *See In re* Application of the United States of America for an Order Relating to Telephones Used by Suppressed, slip op. at 7-8.

217. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010) ("[E]x ante regulation of computer warrants is both constitutionally unauthorized and unwise."). As a policy matter, magistrate judges impose their rules ex parte and with no opportunity for public feedback, and their procedures apply only piecemeal to those applications that come before that particular magistrate.

218. King v. Burwell, 135 S. Ct. 2480, 2489 (2015) (quoting Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2444 (2014)).

219. *King* presented a statutory interpretation question fundamental to the overarching design of the Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code)—whether the tax credits scheme at the crux of health care reform extended to individuals in states with a health care exchange established or operated by the federal government (as opposed to the state). *King*, 135 S. Ct. at 2485. The IRS promulgated a rule interpreting the statute to permit tax credits to such individuals. A majority of the Supreme Court agreed that the statute extended tax credits to those individuals, but it declined to rely on *Chevron* or to otherwise defer to the agency's interpretation. *Id.* at 2489, 2496.

The Second Circuit's decision in *ACLU v. Clapper* might be construed to have adopted a similar conception of Fourth Amendment reasonableness, albeit in dictum.[220] *Clapper* concerned a constitutional and statutory challenge to the NSA's bulk metadata collection program under section 215 of the PATRIOT Act.[221] The Second Circuit resolved the case before it on statutory grounds, holding that section 215 did not authorize the metadata collection program.[222] The court also suggested in dictum, however, that congressional authorization of metadata collection should have bearing on a judicial determination of Fourth Amendment reasonableness.[223] The court emphasized Congress's unique position "to understand and balance the intricacies and competing concerns involved in protecting our national security, and to pass judgment on the value of the telephone metadata program as a counterterrorism tool."[224]

There are powerful, and I think correct, arguments for the proposition that only Congress, not an agency, can create a proactive and preventative metadata collection program inside the United States—and, importantly, that Congress's design of an investigatory subpoena process does not amount to such a programmatic authorization. This is precisely the sort of systemic question that the traditional Fourth Amendment framework obscures because

---

220. 785 F.3d 787, 824 (2d Cir. 2015).

221. The section 215 program was first revealed to the public as a result of leaks from Edward Snowden and sparked immense controversy, a series of critical government reports, multiple court cases, presidential action, and ultimately legislative reform. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (codified at 50 U.S.C. § 1861(b)(2) (2014)) (prohibiting bulk collection by the government); RICHARD A. CLARKE ET AL., PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 10 (2013) [hereinafter PRG REPORT]; PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 1-2 (2014) [hereinafter PCLOB SEC. 215 REPORT]. In the U.S. District Court for the District of Columbia, Judge Leon granted preliminary relief on the ground that the program was constitutionally suspect. But the issue was never decided by the D.C. Circuit, which ultimately dismissed the case as moot. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013) (finding that plaintiffs have a substantial likelihood of showing that the NSA's bulk collection program violates the Fourth Amendment), *rev'd and remanded*, 800 F.3d 559, 561 (D.C. Cir. 2015) (per curiam); Klayman v. Obama, Civ. No. 13-851 (RJL), 2015 WL 6873127 (D.D.C. Nov. 9, 2015) (granting preliminary injunction on remand), *appeal dismissed as moot*, No. 15-5307 (D.C. Cir. Apr. 4, 2016). The program has also, however, been repeatedly reauthorized by the FISC. *See, e.g.*, *In re* Application of the FBI, No. 15-01, 2015 WL 5637562, at *6-13 (FISA Ct. June 29, 2015) (recounting and reaffirming these statutory and constitutional rulings).

222. *See Clapper*, 785 F.3d at 826.

223. *See id.* at 824 ("[W]hether Congress has considered and authorized a program such as this one is not irrelevant to its constitutionality.").

224. *Id.*

it does not see beyond any one-off application of the subpoena authority. For the federal executive to initiate a program of bulk metadata collection involving domestic calls and continue it for a period of years (the program was in place for over a decade[225]), the Fourth Amendment at a minimum requires congressional authorization. This might be just the sort of legal question that Kerr had in mind in proposing a rule of lenity. But statutory ambiguity pervades program design, and a rule of lenity fails to disentangle those types of ambiguity that an agency *should* flesh out through program design (subject to judicial supervision).

The legal authority to engage in a program of surveillance involving domestic communications should come from Congress. But there are myriad legal questions at the level of program design and implementation that we will need to look to agencies to develop in the first instance. Rather than kicking the issue back to Congress every time an ambiguity arises, administrative law suggests a more discerning role for agency elaboration, congressional specification, and judicial review.

The section 702 surveillance program again provides a helpful example. The legal authority to undertake programmatic collection under section 702 is provided in FISA. In contrast to the section 215 program, then, the authorization for the program itself is statutory. This distinction between the two programs should have bearing on the question whether each type of collection is reasonable under the Fourth Amendment. Yet governance of the section 702 program raises a number of difficult and consequential legal questions under the statutory scheme—questions with significant implications for Fourth Amendment reasonableness. Does section 702 permit the collection of multiple-communication transactions, for example, or does it authorize only the collection of discrete communications involving a foreign intelligence target? Given that section 702 is a warrantless collection authority for surveillance directed at non-U.S. persons overseas, what types of searches for specific U.S. persons are permitted in the resulting datasets, and pursuant to what safeguards?

Kicking the statute back to Congress every time such questions arise would run into the difficulties discussed earlier—Congress is simply ill suited to decide every hard legal question that arises from program design and implementation. But relying on agencies to answer these questions in secret or through classified FISC review would raise the very significant concerns that Kerr and others have identified.

Recognizing these concerns in a range of policy settings, administrative law infuses administrative process with requirements for legal and political

225. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 797-801 (2014).

accountability. A transparent and participatory process of rulemaking—administrative law teaches—creates a more deliberative, more legitimate agency-made law.[226] If we are relying on agency-made rules to give meaning to Fourth Amendment reasonableness, then we also need to consider the process by which those administrative rules are developed. Integrating these structural and procedural considerations into Fourth Amendment reasonableness review could achieve a more transparent and participatory approach to surveillance policymaking without looking to Congress to resolve ambiguity at every turn.[227]

B. Shaping Governance Through Evidentiary Exclusion

Judicial deference in constitutional criminal procedure could be conditioned on administrative oversight in another way. The exclusionary rule—the Fourth Amendment's key implementing device—could become a mechanism to incentivize extrajudicial and systemic governance. The germ of the idea is already there in the Court's recent exclusionary rule decisions.

Herring v. United States[228] and *Arizona v. Evans*[229] both concerned arrests based on warrants that were no longer valid. In *Herring*, the defendant was arrested based on a warrant that, unknown to the arresting officer, had been

---

226. *See supra* Part II.C.

227. A different approach suggested in the literature is use of a reinvigorated, albeit modified, nondelegation doctrine to require congressional specification and administrative regulation of policing. *See* DAVIS, DISCRETIONARY JUSTICE, *supra* note 26, at 58; Slobogin, *supra* note 25, at 1724-25; *see also* Friedman & Ponomarenko, *supra* note 25, at 1893-94 (arguing for expanded use of nondelegation doctrine under state law). I am skeptical that separation of powers law, in the form of a nondelegation rule, provides a useful doctrinal mechanism for surveillance governance. First, the nondelegation doctrine applies generally to all administrative conduct, and the concerns with its use to limit affirmative government and institutional innovation are well grounded. *See* Stewart, *supra* note 138, at 1676-88. Second, the nondelegation doctrine focuses on prior authorization—that is, the question whether an agency can make legal policy instead of Congress. It does not consider ongoing oversight given evolving surveillance activities and interconnected administrative actors. Third and relatedly, the nondelegation doctrine asks whether Congress has specified intelligible principles, not whether those limits are constitutionally reasonable in light of the competing interests of privacy and security, as the Fourth Amendment prescribes. As a result, a reinvigorated nondelegation doctrine would provide a limited response to a set of authority-based concerns but at potentially great cost and without facilitating a more comprehensive vision of governance. *See* Simon, *supra* note 30, at 65-66. To the extent that nondelegation concerns are addressed through subconstitutional doctrines of administrative law, however, *see, e.g.*, Cass R. Sunstein, *Nondelegation Canons*, 67 U. CHI. L. REV. 315, 315-16 (2000), I agree that there is value in extending those subconstitutional doctrines to surveillance, *see infra* Part IV.A.

228. 555 U.S. 135 (2009).

229. 514 U.S. 1 (1995).

recalled five months earlier, apparently because it had been issued in error.[230] The Dale County Sheriff's Department had failed to update its warrant database to reflect the recall. In *Evans*, the warrant at issue had been quashed seventeen days prior to the arrest, but the relevant database was not updated because of an error by a clerk of the state court.[231] The majority in both cases held that the exclusionary rule did not apply.[232]

Concurring in *Evans*, Justice O'Connor suggested that the pivotal question was not whether "the police were innocent of the court employee's mistake" but whether they "acted reasonably in their reliance on the recordkeeping system itself."[233] On the facts before the Court, she emphasized, the database error was due to a court employee's divergence from the established recordkeeping protocol.[234] The relevant system of administrative governance was sound, even if it was not entirely error-proof. Justice O'Connor urged, in contrast, that "it would not be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests."[235]

The decisive question for Justice O'Connor was one of administrative governance: What structural and procedural safeguards existed to ensure the veracity of the information provided by the warrant database? Justice O'Connor's approach to the exclusionary rule was both systemic and institutionally grounded. She asked whether administrative structures and processes were in place to create a reliable warrant database, even if the particular warrant at issue had not been correctly expunged.[236]

While *Evans* concerned an error by a clerk of the court, *Herring* presented the Court with a database error by another police officer. The majority in *Herring* again declined to apply the exclusionary rule. To trigger evidentiary exclusion, Chief Justice Roberts wrote for the Court, "police conduct must be

230. *See* 555 U.S. at 149 (Ginsburg, J., dissenting).

231. *Evans*, 514 U.S. at 4.

232. *Herring*, 555 U.S. at 137; *Evans*, 514 U.S. at 6.

233. 514 U.S. at 16-17 (O'Connor, J., concurring) (emphasis omitted).

234. *Id.* at 16.

235. *Id.* at 17 (emphasis omitted).

236. *See id.*; *see also id.* at 18-19 (Stevens, J., dissenting) ("The Amendment is a constraint on the power of the sovereign, not merely on some of its agents. The remedy for its violation imposes costs on that sovereign, motivating it to train all of its personnel to avoid future violations." (citation omitted)); *id.* at 29 n.5 (Ginsburg, J., dissenting) ("Just as the risk of *respondeat superior* liability encourages employers to supervise more closely their employees' conduct, so the risk of exclusion of evidence encourages policymakers and systems managers to monitor the performance of the systems they install and the personnel employed to operate those systems.").

sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."[237] While the majority's approach to deterrence focused on the culpability or recklessness of a particular officer, there is another potential approach to deterrence lurking in *Herring*.[238]

The error at issue in *Herring*, the Court emphasized, was "nonrecurring";[239] cases involving "systemic errors" might warrant a different result.[240] The possibility of systemic error relief did not console the dissent, for how could an "impecunious defendant . . . make the required showing?"[241] It would be exceedingly difficult for a defendant to demonstrate systemic error—an idea that the majority nowhere defined.

But what if the burden were not on the defendant? What if an error in the database required the government, in order to avoid evidentiary exclusion, to demonstrate that extrajudicial mechanisms of oversight and accountability were firmly in place? This approach to deterrence would not focus on the individual officer on the beat, but on the policymaker—that is, the actors in charge of program design and oversight.[242] Using the exclusionary rule to encourage systemic administration would be a more workable, and more institutionally grounded, approach to "systemic errors."

The Court has repeatedly described the exclusionary rule as a remedy of last resort.[243] But it has rejected evidentiary exclusion without meaningfully exploring search and seizure governance. Applying the exclusionary rule in the absence of effective mechanisms for administrative oversight could itself generate the development of those extrajudicial alternatives.

As a mechanism for vindicating Fourth Amendment values, of course, the exclusionary rule remains limited. It depends on specific searches, against particular individuals, that generate evidence for use in a particular criminal

237. *Herring*, 555 U.S. at 144.

238. Deterrence is not the only rationale underlying the exclusionary rule. *See, e.g.*, Richard M. Re, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885, 1894-95 (2014) (offering a detailed critique of the exclusionary rule's normative defenses). But it is today the prevailing justification adopted by the Court. *See id.* at 1894 nn.34-37 (listing cases in which the Court relied on a deterrence rationale); *see also, e.g.*, Davis v. United States, 131 S. Ct. 2419, 2426 (2011).

239. *See Herring*, 555 U.S. at 144.

240. *See id.* at 146 ("In a case where systemic errors were demonstrated, it might be reckless for officers to rely on an unreliable warrant system.").

241. *Id.* at 157 (Ginsburg, J., dissenting).

242. *See* Rappaport, *supra* note 13, at 259 ("Through second-order decisions the Court can 'turn up the heat,' intensifying the deterrent effect of exclusion to pressure political policy makers to promulgate and enforce regulations to control the behavior of the rank and file.").

243. *See Herring*, 555 U.S. at 140; Hudson v. Michigan, 547 U.S. 586, 591 (2006).

trial. And the Fourth Amendment claim must not have been bargained away in the course of plea negotiations.[244] Even when stars align and the exclusionary rule serves up the Fourth Amendment question, the mechanism itself can generate cramped conceptions of the Fourth Amendment's protections. This is because finding a Fourth Amendment violation will often be seen as preventing the use of incriminating evidence against a particular criminal wrongdoer.[245]

Shifting from administrative law-as-analogy to administrative law-as-law reveals an additional mechanism for courts to shape surveillance governance.

IV. Administrative Law as a Complement to Constitutional Criminal Procedure

Rather than merely teaching Fourth Amendment law how to approach the court-agency relationship, administrative law *as law* can create additional opportunities for judicial intervention. Because a variety of surveillance programs have a national nexus, federal administrative law itself can provide a tool to discipline discretion and enhance accountability in the executive's exercise of the search power. This Part first shows how administrative law could enable courts to address gaps in surveillance governance and then explains why administrative law does not currently play this role. To do so, I begin with a stylized account of administrative law—a statutory requirement for notice-and-comment rulemaking. I rely on this classic conception of administrative procedure to show how an administrative law mechanism could help courts respond to the problems posed by aggregation, silos, and spillovers. I then turn to a specific institutional context—the foreign intelligence space—and evaluate an emergent administrative law of surveillance under FISA. Section 702 of FISA provides a valuable case study because it reveals both productive first steps and an unfulfilled promise of administrative law in surveillance governance.

A. Administrative Law's Potential

Administrative procedure typically uses a different point of entry from constitutional criminal procedure: the moment of lawmaking by agencies—that is, the moment when the agency makes binding, legal policy. Because it enables judicial intervention through a different portal, administrative law can

244. *See, e.g.*, Eugene Milhizer, *The Exclusionary Rule Lottery*, 39 U. TOL. L. REV. 755, 764 (2008).

245. This critique of the exclusionary rule is richly developed in the literature. *See, e.g.*, Amar, *supra* note 88, at 793-94; Steiker, *supra* note 88, at 853; William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 912-13 (1991).

create a space for judicial supervision otherwise unavailable under the Fourth Amendment. Administrative law also enables judicial review at the level of program design through policymaking. And it can continue to govern program design over time in response to policy change. Administrative law, in addition, provides a remedy more responsive to the institutionalized search power: it responds to inadequate surveillance policymaking by requiring the agency to refine its consideration of the policy question and available alternatives.[246] Finally, and as others have argued, administrative law brings greater transparency and democratic accountability to agency-made law.[247] In each of these ways, administrative law can help to fill some of the governance gaps created by programmatic surveillance.

1. Aggregation

A core challenge that aggregate search and seizure activity poses for traditional Fourth Amendment law is the question when such activity amounts to a Fourth Amendment "search." As detailed above, this problem arises both because of the ongoing and cumulative nature of collection itself and because of the myriad searches undertaken in already compiled datasets. Instead of a legal framework dependent on a moment in time when surveillance activity becomes a Fourth Amendment search, administrative law orients judicial review around a different trigger: agency lawmaking, that is, the moment in time when agencies make legal rules that determine the search and seizure power on the ground.

Consider the DEA's license-plate-reader program. The separate writings in *Jones*, taken together, support the idea that cumulative and extensive tracking of one's movements can raise Fourth Amendment concerns. But the transactional Fourth Amendment framework makes it very difficult to extend this idea to a program of license plate data collection. When the license plate data are initially acquired, it is through generalized collection that would not be subject to a warrant. And when the license plate data are accessed, it is already information in the government's hands. It therefore does not constitute a "search" under traditional Fourth Amendment law.

A framework statute like the APA could require this type of program design to proceed under a rulemaking requirement, pursuant to principles of transparency, public input, and judicial review. An agency could be required to

246. This can take the form of either "thin" or "thick" rationality review. *See* Jacob Gersen & Adrian Vermeule, *Thin Rationality Review* 2-3 (Harvard Law Sch. Pub. Law Working Paper No. 15-15, 2015), http://ssrn.com/abstract=2639644.

247. *See* DAVIS, POLICE DISCRETION, *supra* note 26, at 106, 112-120 (describing democratic benefits of rulemaking); Friedman & Ponomarenko, *supra* note 25, at 1835 (describing "democracy deficit" in policing and theorizing as to its causes).

specify what types of information would be collected, how long the information would be retained, to what purposes it could be used, and with what agencies information could be shared. Administrative law also could require this type of surveillance rulemaking to address, for instance, whether and under what circumstances individuated searches in the license-plate-reader database require senior-level approval or a showing of individualized suspicion.

It may be that some types of searches in a license-plate-reader database—such as a search that would collect months of detailed data on an individual driver's whereabouts—*should* constitute a "search" under the Fourth Amendment and require a warrant, even though the data are already in the government's hands. But administrative law can supply legal tools to govern this type of surveillance program in contexts short of where the warrant requirement would apply and without requiring a court to determine the precise moment at which cumulative intrusions might amount to a Fourth Amendment "search."

2. Silos and spillovers

Administrative law also could help address the problems of silos and spillovers. Take DNA collection and the question whether to permit a "familial search" policy. As detailed above, this is a type of search practice that enables law enforcement to use an individual's DNA sample to identify that individual's relatives as potential suspects in an investigation.[248] Law enforcement might be interested in investigating those relatives where the DNA sample in the database is not a perfect match to the DNA sample that was found at a crime scene—so the individual who provided DNA is not himself or herself a suspect—but the DNA match is close enough that there is a possibility that the suspect could be a relative of the sampled individual.

248. The underlying premise for familial searching is that family members are more likely than unrelated persons to have similar genetic profiles. The FBI defines familial searching as "a deliberate search of a DNA database conducted for the intended purpose of potentially identifying close biological relatives to the unknown forensic profile obtained from crime scene evidence." *See Familial Searching*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/about-us/lab/biometric-analysis/codis/familial-searching (last visited May 5, 2016). The distinction that the FBI and many states draw between "fortuitously and deliberately discovered partial matches" has been challenged. *See, e.g.*, Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751, 755-56, 772 (2011) (arguing the distinction between fortuitous and deliberate partial matches should be "dismantled" because it "imposes significant structural and transparency costs . . . yet is supported by neither logic nor principle"). For an overview of familial searching, the underlying science, and existing technologies, see MURPHY, *supra* note 112, at 191-96; and Ram, *supra*, at 757-65.

Whether familial searching is "reasonable" under the Fourth Amendment implicates significant and unsettled questions.[249] For example, it raises the question whether law enforcement can make someone a suspect—that is, whether suspicion can be individualized—on the basis of one's familial affiliation to a sampled individual. Yet the transactional framework of Fourth Amendment law creates several barriers to judicial consideration of these questions.

Points of entry again provide one type of barrier, this time as a result of silos. The moment in time when the familial search occurs is a point at which the data are already in the government's hands: the government already has collected the sampled individuals' DNA, and the question is what type of queries can the government now run in the existing DNA databases. For this reason, familial searches in the DNA database may not constitute a "search" under existing Fourth Amendment law.[250]

Spillovers present an additional barrier. The real target of the familial search is not the individual whose DNA was sampled. Instead, it is the relative of the sampled individual. Imagine an arrestee named Sally whose DNA is sampled and added to the national DNA database, CODIS. Law enforcement runs DNA collected from a recent crime scene against the DNA samples in CODIS and finds no perfect match. Law enforcement then decides, pursuant to a familial search policy, to look for a partial match in the database. The agency runs the search and finds a partial match with Sally's DNA sample. Law enforcement knows that Sally is not the right suspect for the unsolved crime (hers is not a perfect match with the DNA found at the crime scene). But the suspect might be someone who shares some biological markers with Sally; it might be her sibling, Joe.

Joe, however, lacks a clear path to challenge the familial search policy under Fourth Amendment law. This is because the physical intrusion that took place was not a search done *to Joe*. The DNA sample in the database was collected from Sally. And so Joe probably lacks Fourth Amendment standing to challenge the familial search policy.[251] The aggregate implications of a familial

249. For an important account of the legal and policy concerns with familial searching, see MURPHY, *supra* note 112, at 189-214.

250. *See, e.g.*, Johnson v. Quander, 440 F.3d 489, 498 (D.C. Cir. 2006) ("[A]ccessing the records stored in [a government database] is not a 'search' for Fourth Amendment purposes. As the Supreme Court has held, the process of matching one piece of personal information against government records does not implicate the Fourth Amendment."). *But see* MURPHY, *supra* note 112, at 210 (recognizing these doctrinal obstacles but proposing path to doctrinal reform).

251. *See* United States v. Mitchell, 652 F.3d 387, 409 n.19 (3d Cir. 2011). Scholars have proposed changes to this doctrinal limitation by analogy to property law and Fourth Amendment cases involving consent to search under circumstances of shared tenancy.
footnote continued on next page

search policy also do not find a ready hook in existing Fourth Amendment law. Under the transactional framework, there is little space for courts to undertake a systemic evaluation of how familial searches affect certain subpopulations of which Joe is a part. For example, because more persons of color are arrested and therefore sampled, familial search policies may disproportionately burden communities of color.[252] Finally, because traditional Fourth Amendment law focuses on the one-off intrusion rather than policymaking, it permits familial search policies designed in secret, without participatory opportunities or even clear visibility into who is making what decisions.

Currently, the FBI does not conduct familial searching using the Combined DNA Index System (CODIS), but the adoption of familial search policies at the state and local levels illustrates the point.[253] These familial search policies today range from a few public policies approved by a state attorney general to unpublished policies contained in forensic laboratory manuals or even unwritten policies used to guide forensic lab work.[254] Most jurisdictions do not have public and accessible policies around familial searching.[255] The few familial search policies adopted publicly and by politically accountable officials provide some important safeguards. California's policy, adopted through a public memorandum from the state's attorney general, limits the use of familial searching to a last resort and only in violent crime investigations raising significant public safety concerns, and it subjects the release of a familial search

See MURPHY, *supra* note 112, at 209; Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 919-29 (2015).

252. In a now-superseded judicial opinion, the California Court of Appeal explained that "familial DNA searches have a discriminatory effect" because they "condition criminal suspicion on nothing more than the fact of being a close relative of a person whose profile is in the DNA database, and racial and ethnic minorities comprise a much greater portion of that database than their proportion in the population at large." People v. Buza, 180 Cal. Rptr. 3d 753, 790 (Ct. App. 2014), *review granted*, 342 P.3d 415 (Cal. 2015).

253. The FBI did conduct rulemaking to adopt a policy to collect DNA samples from arrestees. In response to comments provided during that rulemaking, the FBI noted that it does not currently conduct familial searching. *See* DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. 74,932, 74,938 (Dec. 10, 2008) (to be codified at 28 C.F.R. pt. 28). There have been calls for the FBI to begin conducting familial searching and efforts to improve the technological capacity of CODIS to facilitate these types of searches. *See* MURPHY, *supra* note 112, at 197-98.

254. *See* MURPHY, *supra* note 112, at 190; OFFICE OF INVESTIGATIVE & FORENSIC SCIS., NAT'L INST. OF JUSTICE, FAMILIAL DNA SEARCHING: CURRENT APPROACHES 1 (2015) [hereinafter NIJ FAMILIAL SEARCHING REPORT].

255. *See* Ram, *supra* note 248, at 776-78 (finding that "[m]ost jurisdictions have refrained from prescribing rules governing partial matching in easily accessible formats" and "[n]early all written state policies are available only in internal lab manuals").

result to supervisory review and approval.[256] Most informal policies contained in lab manuals lack these kinds of constraints, and often the policy itself is very difficult to locate.[257] Every state effort to obtain express statutory authorization to conduct familial searching has failed.[258] Though a number of states conduct familial searching, none of their policies is explicitly authorized by statute.[259]

The FBI initially prohibited participating federal, state, and local agencies from using the federal DNA database program to share information about partial DNA matches—effectively preventing familial searching in CODIS across jurisdictions.[260] Under especially vocal opposition to that policy from the Denver District Attorney, the FBI changed its policy to allow participating jurisdictions to decide whether to conduct familial searching or to share partial match results discovered through CODIS.[261] The FBI made the change informally through a CODIS "bulletin," and it has not imposed obligations on states that conduct familial searching to do so pursuant to a transparent policy.[262]

Now consider review of a familial search using the doctrinal tools of administrative law. The entry point for a court would turn not on the moment of search but on the moment of administrative lawmaking—that is, the policy decision to permit familial matching in a DNA database. Administrative law could require a transparent decision by law enforcement to authorize familial

256. *See* Div. of Law Enf't, Cal. Dep't of Justice, Information Bulletin No. 2008-BFS-01, DNA Partial Match (Crime Scene DNA Profile to Offender) Policy 1-2 (2008), http://ag.ca.gov/cms_attachments/press/pdfs/n1548_08-bfs-01.pdf; *see also* NIJ FAMILIAL SEARCHING REPORT, *supra* note 254, app. H.

257. *See* Ram, *supra* note 248, app. B at 812 (comparing investigation-related protections under different states' policies); *see also id.* at 766, 776-77.

258. *See* NIJ FAMILIAL SEARCHING REPORT, *supra* note 254, at 11 ("No state that has sought explicit statutory authorization [to conduct familial searching] has been successful in obtaining it."). Efforts in Congress to require the FBI to conduct familial searching also have not succeeded. *See* Utilizing DNA Technology to Solve Cold Cases Act of 2011, H.R. 3361, 112th Cong. (2011).

259. *See* NIJ FAMILIAL SEARCHING REPORT, *supra* note 254, at 11.

260. *See* MURPHY, *supra* note 112, at 190 ("FBI rules at the time forbade states from disclosing to other states the identifying information of anyone other than the 'putative perpetrator.'").

261. *See* Fed. Bureau of Investigation, CODIS Bulletin BT072006, Interim Plan for Release of Information in the Event of a "Partial Match" at NDIS (2006) [hereinafter 2006 Interim Plan]; *see also* MURPHY, *supra* note 112, at 190.

262. *See* 2006 Interim Plan, *supra* note 261. The FBI's final Plan for the Release of Information in the Event of a Partial Match at NDIS is included as an appendix to the National DNA Index System Operational Procedures Manual. *See* FBI LABORATORY, NATIONAL DNA INDEX SYSTEM (NDIS) OPERATIONAL PROCEDURES MANUAL app. G at 74-76 (2013).

searching, a decision informed by public comment. And the agency's decision could be challenged in court. Because the agency's decision would be more transparent, it would be more amenable to a challenge for consistency with the underlying statutory scheme.[263] And violation of the underlying statutory scheme would be a clear violation of administrative law, in contrast to the existing Fourth Amendment framework.

Administrative law also could supply a governance method more responsive to spillovers. We might want to consider, for instance, whether familial searching is used as a last resort and only in connection to particular crimes, how reliable the technology is, and what safeguards are in place to govern its uses.[264] These considerations appear to have informed the few transparent and politically accountable familial search policies adopted to date.[265]

Administrative law might also enable courts to exercise a substantive check under the Fourth Amendment at a more programmatic level—that is, at a level of analysis distinct from the one-off interaction that traditionally governs courts' Fourth Amendment inquiry. We might find, for example, that the familial search policy exacerbates racial disparities in the criminal justice system and arbitrarily creates suspicion based on familial ties.[266] Whether and how these programmatic dimensions implicate the substantive Fourth Amendment right depend on its underlying values. But the point here is that administrative law, as a vehicle for presenting search and seizure policies to courts, could in turn help courts engage in substantive Fourth Amendment review at this very different level of analysis.

Finally, the interconnecting protocols governing familial searches at the federal and state levels highlight an additional way that federal administration might impose greater transparency and accountability on programmatic surveillance. The FBI, for instance, could require participating state and local agencies to comply with certain procedural protections if they choose to use federal funds or national databases to run familial searches. The suggestion raises a variety of considerations that are outside the scope of this Article. But it

263. *See, e.g.*, Murphy, *supra* note 95, at 326 ("Familial search policies represent an end run around database inclusion statutes in several ways: they widen the size of databases by effectively including relatives within them; they widen the types of testing conducted on DNA samples by undertaking additional forms of genetic typing; and they widen the scope of information exposed by the 'junk' DNA the government collects. Yet all of these expansions occur in the shadow, rather than the glare, of the public eye." (emphasis omitted)).

264. *See id.* at 303-09.

265. *See* sources cited *supra* note 256.

266. *See* Murphy, *supra* note 95, at 305, 321-25.

highlights an important direction to extend the administrative framework in future work.

3. Administrative law's absence

Administrative law, then, could help address governance gaps created by programmatic surveillance. And yet, administrative law's governing framework statute, the APA, has not generally been extended to surveillance for a variety of statutory and doctrinal reasons.[267] The statutory text itself provides some exceptions, such as exempting foreign affairs functions from the rulemaking requirements.[268] But more broadly, the statute ties the rulemaking requirement to "agency action" that takes the form of a legislative rule. Those procedural requirements do not extend to other types of agency policymaking such as interpretive rules contained in guidance documents.[269] The distinction is famously murky,[270] but the legislative-rule criterion has operated to exclude many law enforcement- and surveillance-related documents.[271] Recent case law, meanwhile, has limited the types of administrative conduct that fall within the term "agency action," making it more difficult to use the APA to

267. For a discussion of statutory and doctrinal barriers to extending the APA to national security policymaking, see Adrian Vermeule, *Our Schmittian Administrative Law*, 122 HARV. L. REV. 1095, 1112-13 (2009). Vermeule argues that the structure of administrative law insulates executive decisionmaking in the context of emergencies and that this development is inevitable. My claim is that surveillance lawmaking by agencies is generally not about emergencies. It is a routine, ongoing facet of the modern administrative state. In this sense, surveillance governance should not be conceptualized through the law of emergencies. That said, many of the explicit and implicit exemptions that Vermeule identifies extend, formally or in practice, to surveillance policymaking as well under current law.

268. *See* 5 U.S.C. § 553(a)(1) (2014).

269. *See id.* § 553(b)(3)(A).

270. *See, e.g.*, David L. Franklin, *Legislative Rules, Nonlegislative Rules, and the Perils of the Short Cut*, 120 YALE L.J. 276, 286-87 (2010) ("Courts have described the tests that govern these cases as 'fuzzy,' 'tenuous,' 'blurred,' 'baffling,' and 'enshrouded in considerable smog.'" (footnotes omitted)). Some scholars have argued that, rather than parse legislative from nonlegislative rules on substantive grounds, courts should "invert" the test: a rule should be considered "legislative" if it is promulgated through notice-and-comment proceedings. *See, e.g.*, Jacob E. Gersen, *Legislative Rules Revisited*, 74 U. CHI. L. REV. 1705, 1718-21 (2007); *see also* William Funk, *A Primer on Nonlegislative Rules*, 53 ADMIN. L. REV. 1321 (2001); John F. Manning, *Nonlegislative Rules*, 72 GEO. WASH. L. REV. 893, 929 (2004). Others have recognized the difficulties of the courts' contextualized substantive approach but embraced it as valuable. *See* Franklin, *supra*, at 678-79.

271. *See* Friedman & Ponomarenko, *supra* note 25, at 1845-46 (discussing the exclusion of policing documents from the legislative rule category). For a more general discussion of the status of guidance documents with respect to the APA's "legislative rule" categorization, see Mark Seidenfeld, *Substituting Substantive for Procedural Review of Guidance Documents*, 90 TEX. L. REV. 331 (2011).

address programmatic dimensions of administration.[272] Thus, while administrative law has long been the product of judicial elaboration, often in the shadow of constitutional values, current doctrinal development impedes its reach into surveillance governance.

A decision from the D.C. Circuit, the court of appeals with primary responsibility for the elaboration of federal administrative law, nevertheless gestures at the possibility of using administrative law to govern surveillance. In *Electronic Privacy Information Center v. U.S. Department of Homeland Security* (*EPIC*), the D.C. Circuit considered an APA challenge to the Transportation Security Administration's (TSA) decision to screen airline passengers using "advanced imaging technology" (or body scanners) instead of metal detectors.[273] Body scanners create an image of an unclothed person, which then allows the operator to detect things like liquid or powder that a metal detector would not detect. The Electronic Privacy Information Center and two individuals sued the TSA, arguing that the agency had failed to comply with the APA because it did not adopt the new search policy pursuant to notice-and-comment rulemaking.[274] The D.C. Circuit agreed.[275]

EPIC suggests one way that courts could amplify their supervision of surveillance policymaking using administrative law. A key question in the case was whether the new policy constituted a legislative rule. The D.C. Circuit viewed the distinction between legislative and nonlegislative rules pragmatically. The difference, the court explained in *EPIC*, is "'one of degree' depending upon 'whether the substantive effect is sufficiently grave so that notice and comment are needed to safeguard the policies underlying the APA,'" and it characterized those underlying policies as "serv[ing] 'the need for public participation in agency decisionmaking.'"[276] The court concluded that the new TSA search policy "affects the public to a degree sufficient to implicate the policy interests animating notice-and-comment rulemaking."[277] The rule at issue bound the agency and the public, and it "substantially change[d] the experience of airline passengers."[278] In so holding, the court emphasized the privacy concerns that had been raised by the new search technology, and it suggested that the broad application of the search technology was, if anything,

272. *See* ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007); Norton v. S. Utah Wilderness All., 542 U.S. 55, 72 (2004); *see also* Vermeule, *supra* note 267, at 1109-12.

273. 653 F.3d 1, 2-3 (D.C. Cir. 2011).

274. *Id.* at 3.

275. *Id.*

276. *Id.* at 5-6 (first quoting Lamoille Valley R.R. Co. v. Interstate Commerce Comm'n, 711 F.2d 295, 328 (D.C. Cir. 1983); then quoting Chamber of Commerce v. U.S. Dep't of Labor, 174 F.3d 206, 211 (D.C. Cir. 1999)).

277. *Id.* at 6.

278. *Id.* at 7.

a reason for closer scrutiny with the APA's procedural safeguards.[279] The court remanded the rule to the agency for notice-and-comment proceedings but, for security reasons, allowed the new policy to remain in operation while those proceedings were pending.[280]

There are two types of administrative procedure at issue in a case like *EPIC*. The first type is designed to safeguard substantive Fourth Amendment interests. In *EPIC*, these rules included, for example, requirements that the agency "distort[] the image created using [the body scanner] and delet[e] it as soon as the passenger has been cleared."[281] The second type of administrative procedure is the process that the agency uses to arrive at those protections. Only the first type of process is relevant under the traditional Fourth Amendment test. Indeed, *EPIC* itself considered only this first type of administrative constraint when it resolved the plaintiffs' Fourth Amendment challenge to the body scanners.[282]

Yet one way to understand the ruling in *EPIC* is that administrative rules that, in effect, balance substantive Fourth Amendment interests should be subject to the structural protections of transparency and participatory process. When confronted with Fourth Amendment decisionmaking *through* administrative procedure, the court imposed the APA's structural safeguards. *EPIC* thus suggests the possibility of using subconstitutional doctrines of

279. *See id.* at 6-7.

280. *Id.* at 8. By keeping the then-current policy in place with no expiration, the D.C. Circuit arguably diminished the force of its own ruling, and the TSA was slow to implement the court's ruling. The TSA held a notice-and-comment period, receiving extensive comments on the body scanners, including many submissions concerning privacy and the body scanner technology. *See, e.g.*, Pride Found., Comment Letter on Notice of Proposed Rulemaking Regarding Passenger Screening Using Advanced Imaging Technology, Docket No. TSA-2013-0004 (June 24, 2013), http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-4519 (noting, inter alia, the effects of advanced imaging technology on transgender individuals' privacy in smaller communities where they may know the TSA personnel); U.S. Justice Found., Comment Letter on Notice of Proposed Rulemaking Regarding Transportation Security Administration: Use of Dangerous Body Scanners, Invasive Patdowns, and Other Abuses of Constitutional Rights, Docket No. TSA-2013-0004 (July 2, 2013), http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-5292 (commenting on privacy and technological concerns). But the agency delayed promulgation of the new rule, and it ultimately took renewed litigation and a writ of mandamus to prompt it. *See* Order, *In re* Competitive Enter. Inst., No. 15-1224 (D.C. Cir. Oct. 23, 2015). The final rule issued as this Article went to print. *See* 81 Fed. Reg. 11,364 (Mar. 3, 2016) (to be codified at 49 C.F.R pt. 1540).

281. 653 F.3d at 10.

282. *See id.* (finding no Fourth Amendment violation).

administrative law to enable courts to supervise and impose procedural protections on agency implementation of the Fourth Amendment.[283]

Understanding *EPIC* on these terms, however, raises serious questions under two strands of current Supreme Court case law. Those cases cast significant doubt on, if they do not currently foreclose, this more integrated constitutional-administrative law framework.[284] The Court, first, has rejected the idea that a more stringent standard of review should apply under the APA "to agency actions that implicate constitutional liberties."[285] In *FCC v. Fox Television Stations, Inc.*, the Federal Communications Commission (FCC) changed its enforcement policy governing the broadcasting of indecent language.[286] The broadcasters—echoed by four Justices in dissent—argued that the agency's policy shift should be subject to more searching review than other instances where an agency changes policy course because here the policy at issue implicated First Amendment concerns.[287] A majority of the Court, in an opinion by Justice Scalia, rejected this view. The APA already permits courts to set aside constitutionally unlawful agency action, Justice Scalia emphasized.[288] But courts, he wrote, could not calibrate *administrative law* standards of review to accommodate constitutional considerations.[289]

In a separate line of cases, the Supreme Court has rejected the D.C. Circuit's creation of procedural requirements beyond those specified in the APA. Most recently, in *Perez v. Mortgage Bankers Ass'n*, the Court repudiated a doctrinal rule adopted by the D.C. Circuit that required an agency to use notice-and-comment rulemaking when it issues a new interpretation of a regulation that deviates significantly from a previously adopted interpretive rule.[290] The Court found that this doctrine was inconsistent with the plain text of the APA,

283. *See* Metzger, *supra* note 14, at 1843-44 (identifying a "porous boundary between constitutional and subconstitutional law, with statutory or administrative law disputes increasingly functioning as mechanisms for constitutional articulation").

284. *See* Metzger, *supra* note 187, at 484 (arguing against a sharp division between constitutional law and administrative law but explaining why current doctrine is inconsistent with this approach); *cf.* Michael Coenen, *Constitutional Privileging*, 99 VA. L. REV. 683, 684 (2013) (describing and critiquing the courts' practice of "extend[ing] specialized forms of procedural or remedial treatment to claims involving constitutional law").

285. FCC v. Fox Television Stations, Inc., 556 U.S. 502, 516 (2009).

286. *Id.* at 511-12.

287. *See id.* at 556 (Breyer, J., dissenting) ("[T]he FCC works in the shadow of the First Amendment, and its view of the application of that Amendment . . . directly informed its initial policy choice. Under these circumstances, the FCC's failure to address this 'aspect' of the problem calls for a remand to the agency.").

288. *See id.* at 516-17 (majority opinion) (discussing 5 U.S.C. § 706(2)(A)).

289. *See id.*

290. 135 S. Ct. 1199, 1203 (2015).

which expressly excludes "interpretive rules" from the notice-and-comment requirement.[291]A core reason for the D.C. Circuit's approach had been the pragmatic concern that, absent such a constraint, agencies would adopt broad interpretive rules and then reinterpret them, thus circumventing the APA's structural protections. The Supreme Court rejected the D.C. Circuit's extension of the notice-and-comment requirement to the interpretive context. In so holding, the Court reaffirmed longstanding precedent holding that courts lack common law power to impose new procedural requirements on agencies.[292] In *Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, Inc.*, the Supreme Court had halted a decade-long effort by the D.C. Circuit to create or foster the development of rulemaking requirements beyond those contained in the APA and the agencies' organic statutes.[293]

The Court in *Vermont Yankee* expressly reserved the question whether the Constitution constitutes a separate source of law on which courts may base procedural requirements.[294] And the question of what constitutes a "legislative rule" under the APA was not at issue in either *Fox* or the *Vermont Yankee* line of cases. Yet both doctrinal threads advance themes of judicial restraint that can be understood to cut against the reading of *EPIC* suggested here.[295]

At the same time, the argument elaborated in this Article—that administrative safeguards are essential to protect Fourth Amendment values in a time of programmatic surveillance and that agencies must have a laboring oar in that project—also harmonizes with some of the comparative institutional considerations underlying *Vermont Yankee* and *Perez*.[296] Administrative law—by coupling administrative innovation with a set of procedural and structural checks—can help Fourth Amendment law better utilize the agencies' unique competencies while guarding against their potential overreach. In this way,

---

291. *Id.* at 1206.

292. *See* Vt. Yankee Nuclear Power Corp. v. Nat. Res. Def. Council, Inc., 435 U.S. 519, 524 (1978); *see also* Cass R. Sunstein & Adrian Vermeule, *Libertarian Administrative Law*, 82 U. CHI. L. REV. 393, 397 (2015) (discussing *Vermont Yankee*'s "narrow, black-letter meaning . . . that courts lack common-law power to require agencies to use procedures not mandated by statutes or the Constitution" and the case's "broader meaning . . . that courts are to respect the constitutional allocation of policymaking competence").

293. *See* Antonin Scalia, *Vermont Yankee: The APA, the D.C. Circuit, and the Supreme Court*, 1978 SUP. CT. REV. 345, 345.

294. *See* 435 U.S. at 542-43, 542 n.16.

295. *See, e.g.*, Adrian Vermeule, *Deference and Due Process*, 129 HARV. L. REV. 1890, 1912-13 (2016).

296. Adrian Vermeule, for instance, argues that agencies play an important role in the formation and application of procedural due process law, creating a situation in which courts explicitly or implicitly defer to agencies' due process determinations. *See id.* at 1891; *see also* Bertrall L. Ross II, *Embracing Administrative Constitutionalism*, 95 B.U. L. REV. 519, 523 (2015) (arguing that agencies are comparatively well adapted to interpret vague constitutional texts according to changing societal contexts).

administrative law could be a valuable complement to constitutional rights-based adjudication.[297]

Developing administrative law in this way also would provide a laboratory of experimentation for bringing the Fourth Amendment into the digital age. We typically think of states as the laboratories in our federalist system.[298] But judicial review of federal administration also provides a locus for experimentation.[299] As a site for judicial innovation, administrative law affords federal courts not only an opportunity to experiment with doctrinal answers. There is also value simply in having variegated mechanisms through which courts can work through complex and challenging Fourth Amendment questions. Administrative law could provide a space for judicial engagement with the Fourth Amendment independent of, and freed of some of the limitations that inhere in, the exclusionary rule.

B. Lessons from (and for) the FISC

Section 702 of FISA reflects an emergent administrative law of intelligence.[300] The statute requires FISC review of the administrative rules governing surveillance, including the effect of those rules—at the level of program design—on Fourth Amendment interests.[301] While the legal authority under section 702 authorizes surveillance directed at non-U.S. persons overseas—a category of persons understood to fall outside of the Fourth Amendment's coverage[302]—the legislative provisions also require the court to consider the Fourth Amendment interests implicated as a result of spillovers. Section 702 requires the Attorney General, in consultation with the Director of National Intelligence, to adopt "minimization procedures" to protect U.S.-person interests, and it requires the FISC to review those procedures, as well as "targeting" procedures, for compliance with the statute

297. *See* Metzger, *supra* note 187, at 519-25 (arguing that enforcement of constitutional norms through administrative law would complement other forms of constitutional enforcement by incentivizing agency deliberation about constitutional concerns regarding their decisions).

298. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting); *see also, e.g.*, Arizona v. Evans, 514 U.S. 1, 24 (1995) (Ginsburg, J., dissenting).

299. For an argument that federal administrative policymaking is itself a site of experimentation, see Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267 (1998).

300. This argument is developed in Renan, *supra* note 158.

301. *See* 50 U.S.C. § 1881a(d)-(e), (i)(3)(A) (2014).

302. *See* sources cited *supra* note 59 (discussing territorial nexus of Fourth Amendment doctrines).

and with the Fourth Amendment.[303] Section 702 thus creates a process for administrative rule creation, pursuant to congressional authorization and subject to ongoing FISC review and rigorous internal oversight. Because the legal silo separating "foreign" collection and "domestic" communications no longer tracks technological, sociological, or organizational practice, this administrative law of intelligence is what today instantiates the Fourth Amendment's protections.

Yet section 702 relies on administrative law to protect Fourth Amendment values without the structural protections of transparency, participatory process, and adversarial judicial review that administrative lawmaking ordinarily requires.[304] So while the statutory framework and the intelligence court implicitly have embraced an idea of administrative lawmaking as constitutive of Fourth Amendment reasonableness, they have not developed a sustainable approach to this emergent administrative law. The FISC is relying on administrative rules to do crucial work to give content to Fourth Amendment reasonableness but without the structural conditions that have come to legitimate agency lawmaking elsewhere in the administrative state. Until very recently, the FISC's oversight of section 702 operated almost exclusively in secret, preventing any public accounting of the program's design. Recent legislation and executive branch policy have taken some important steps toward greater disclosure. Yet the program still operates pursuant to only partial and discretionary disclosure and largely nonadversarial judicial review.[305]

Even as section 702 fails to realize the promise of a Fourth Amendment administrative framework, however, its system of governance goes considerably further than most other surveillance programs. Intelligence activities implemented under Executive Order 12,333,[306] for example, are governed by minimization rules developed exclusively inside the executive

303. Minimization procedures have long been a part of FISA. But whereas under other FISA provisions, minimization rules complement a more warrant-like process of review by the FISC itself, administrative rules form the core set of protections under section 702. *See* Renan, *supra* note 158, at 128.

304. *See id.* at 132-34.

305. The recently enacted USA FREEDOM Act of 2015 has taken some steps to make FISC decisionmaking more visible and to create limited opportunities for contested adjudication. The statute provides for the appointment of amicus curiae under certain conditions at the discretion of a FISC judge. And it mandates declassification review for the FISC's significant legal interpretations. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 401-02, 129 Stat. 268, 279-82 (codified at 50 U.S.C. §§ 1803, 1871-72).

306. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

branch, without FISC or any other judicial review.[307] Some of those rules remain classified, and many have not been updated in decades notwithstanding considerable changes to the relevant technologies and operational practice.[308] Outside of the intelligence space, programmatic surveillance appears to have developed with even less interbranch oversight. The DEA's program of metadata collection relating to drug trafficking and its national license-plate-reader initiative are just two examples.[309]

One response might be that surveillance depends on secrecy, a value antithetical to administrative law's guiding principles. This argument could take two forms. The first is that surveillance will be ineffective if it is not conducted surreptitiously. The second is that transparent surveillance policymaking might lead to less surveillance in ways that ultimately threaten national security and public safety interests. These arguments have been especially sticky in connection to foreign intelligence.[310]

Such calls for secrecy fail, however, to grapple with changes in the FISC's institutional role.[311] The FISC was originally designed around a warrant framework.[312] The FISC's role was to review warrant-like applications for surveillance against a particular target and to determine whether FISA's

307. For a more detailed discussion of these aspects of Executive Order 12,333, see Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SECURITY J. 112, 124-33 (2015).

308. *See* Letter from David Medine, Chairman, Privacy & Civil Liberties Oversight Bd., to Attorney Gen. Eric H. Holder Jr. and James R. Clapper, Dir., Office of the Dir. of Nat'l Intelligence (Aug. 22, 2013), https://www.pclob.gov/library/Letter-DNI_AG_12333_Guidelines.pdf ("The Privacy and Civil Liberties Oversight Board has learned that key procedures that form the guidelines to protect 'information concerning United States persons' have not comprehensively been updated, in some cases in almost three decades, despite dramatic changes in information use and technology."). The Privacy and Civil Liberties Oversight Board is currently conducting a review of surveillance activities conducted under Executive Order 12,333. *See* Privacy & Civil Liberties Oversight Bd., PCLOB Examination of E.O. 12333 Activities in 2015, https://pclob.gov/library/20150408-EO12333_Project_Description.pdf.

309. The limited information available about these programs emerges from leaks and Freedom of Information Act releases. But it is impossible on the available public record to piece together a holistic picture of these programs and how they are governed.

310. *See* David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y 209, 281 (2014).

311. *See* Renan, *supra* note 158, at 128. For an argument that the FISC's changed institutional role raises Article III concerns and that those concerns could be "ameliorated through more regular participation by a 'special advocate,'" see Stephen I. Vladeck, *The FISA Court and Article III*, 72 WASH. & LEE L. REV. 1161, 1164 (2015).

312. *See* Kerr, *Rule of Lenity*, *supra* note 132, at 1513-14; Renan, *supra* note 158, at 127-28.

modified probable cause requirement was satisfied.[313] That warrant framework presupposes that the work of lawmaking has happened elsewhere—that the legal ground rules are already in place when the magistrate judge applies them.[314] As with any warrant process, the FISC proceedings were to be ex parte and secret. Yet a core function of the FISC today is also to review federal lawmaking by agencies. Rather than approve individualized probable cause assessments, the FISC in this role is reviewing the administrative policies that create the legal architecture for surveillance. And the FISC reviews those rules for compliance with the underlying statute (FISA) and the Fourth Amendment.[315] Questions such as whether section 702 authorizes the collection of MCTs, or whether and under what conditions the FBI may search for specific U.S. persons in the section 702 datasets—these sorts of decisions constitute the modern law of surveillance. And when those legal rules form the basis of the FISC's Fourth Amendment reasonableness analysis, they make the constitutional law of surveillance.

As I explain elsewhere, "The benefits of secrecy in the intelligence context also need to be traded off against the costs of disclosure (through leaks and other means) that the government cannot control or predict."[316] And as others have written, important developments are diminishing "the half-life of secrets."[317] The choice today may be less about secrecy versus transparency and more about the when and how of transparency.

Redrawing the lines between secrecy and transparency is sure to raise complex questions about how to make the legal framework for surveillance more visible and accessible while protecting classified sources and methods. It may be, for example, that the legal framework governing agency *access* to data (the program's minimization procedures) will be more amenable to a transparent administrative process than the legal rules governing *acquisition*, where that acquisition implicates classified means of collection.[318] I also do not suggest that a mechanical extension of notice-and-comment requirements is

313. For a detailed comparison of FISA's warrant requirements and ordinary Title III warrant requirements, see DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS §§ 11.7-11.10 (West 2015).

314. *See, e.g.*, Kerr, *Rule of Lenity*, *supra* note 132, at 1517.

315. *See, e.g.*, *id.* at 1525-27; Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), http://nyti.ms/1525ElU; *see also* Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 STAN. J. INT'L L. 69, 75 (2015).

316. This discussion is taken from Renan, *supra* note 158, at 135.

317. *See* PETER SWIRE, NEW AM. CYBERSECURITY INITIATIVE, THE DECLINING HALF-LIFE OF SECRETS AND THE FUTURE OF SIGNALS INTELLIGENCE 1-4 (2015), https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/Swire_DecliningHalf-LifeOfSecrets.f8ba7c96a6c049108dfa85b5f79024d8.pdf.

318. For a discussion of data acquisition under the Fourth Amendment, see Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547-64 (2005).

the optimal mechanism to enhance transparency and democratic input into administrative surveillance law.[319] But the secrecy-transparency balance that has long shrouded the law of surveillance on the ground warrants careful recalibration.[320]

Making the overarching legal framework of surveillance programs more visible and participatory may make those programs more resilient.[321] A more visible process of surveillance lawmaking by agencies might ultimately be more acceptable to the public in part because it would lead to a substantively different surveillance law. Agencies preparing for a public accounting of their legal rules do appear to act differently than agencies preparing for a secret assessment.[322] If this is a cost, it is a cost of democratic governance. It might also be, however, that by making surveillance lawmaking by agencies more transparent and accountable, we will put it on sounder footing in the long run.

This raises a different possible objection. One might argue that a more integrated administrative Fourth Amendment framework will legitimate the modern surveillance state in ways ultimately threatening to the Fourth Amendment's underlying values. Given technological, sociological, and political realities, I am skeptical that we can put programmatic surveillance back in the bottle—or that eliminating programmatic surveillance across the board is the right goal for legal reform.[323] To be sure, there are crucial

---

319. *See* Adam B. Cox & Cristina M. Rodríguez, *The President and Immigration Law Redux*, 125 YALE L.J. 104, 219 (2015) ("Some form of public input into the development of enforcement priorities with more formality than private meetings convened by the Executive and less than notice-and-comment rulemaking would be a valuable contribution to regulatory spheres in which the enforcement power drives application of the law, as well as the politics and substantive policy of the area.").

320. In Part V below, I propose a different institutional design to improve transparency and accountability of intelligence programs.

321. *See, e.g.*, PRG REPORT, *supra* note 221, at 125. The recently enacted USA FREEDOM Act begins to reframe the secrecy-transparency tradeoff in foreign intelligence lawmaking, though its interventions remain limited.

322. Indeed, this has led some scholars and policy analysts to urge the intelligence agencies to adopt the "front-page rule" in making surveillance decisions, "at least in the specific context of communications intelligence that takes place in the homeland or that affects US persons abroad." Jack Goldsmith, *A Partial Defense of the Front-Page Rule*, HOOVER INSTITUTION (Jan. 29, 2014), http://www.hoover.org/research/partial-defense-front-page-rule (capitalization altered) (emphasis omitted); *see also* PRG REPORT, *supra* note 221, at 170; SWIRE, *supra* note 317, at 5-7. *But see* Walter Pincus, *'Front-Page Rule' Is Unprecedented in U.S. Intelligence Community*, WASH. POST (Dec. 25, 2013), http://wpo.st/wMyW1. *See generally* PRG REPORT, *supra* note 221, at 170 (explaining that the "Front-Page Rule" is an "informal precept, long employed by the leaders of US administrations, . . . that we should not engage in any secret . . . activity if we could not persuade the American people of the necessity and wisdom of such activities were they to learn of them as the result of a leak or other disclosure").

323. *See* WITTES & BLUM, *supra* note 113, at 185, 196.

questions to be asked about what types of surveillance programs are appropriate, what safeguards are and should be in place, and what the boundaries of a programmatic surveillance power should be. But a more integrated judicial-administrative system will better equip us to address them.

V. Institutionalizing the Fourth Amendment Through Agency Design

The foregoing raises a crucial consideration: not every surveillance program is reasonable to undertake. Even if a one-off interaction would comply with the Fourth Amendment, the program as a whole may have systemic costs that outweigh its benefits—costs that cast doubt on the reasonableness of the program as a whole.[324] Whether to initiate, and whether to continue, a surveillance program is a determination that implicates systemic tradeoffs and requires a holistic understanding of the structural, procedural, and technological safeguards in place. This type of Fourth Amendment reasonableness review seems to call for a consideration of *programmatic efficacy*. The effectiveness of a surveillance program—whether the program is valuable, given its stated goals—is inextricably connected to the question of interest balancing—that is, whether the privacy costs are worth the security gains.[325] This is not to suggest that an effective program is always reasonable under the Fourth Amendment. But an inefficacious one should raise constitutional concerns. And yet, courts have been reluctant to evaluate programmatic efficacy under the Fourth Amendment.

Programmatic efficacy review by an administrative actor, designed with some remove from both the front-line surveillance agencies and the White House, could help to institutionalize this element of Fourth Amendment reasonableness while also creating opportunities for greater transparency and ongoing democratic input in surveillance governance. Enhancing this type of agency design, in turn, might enable courts to better supervise programmatic efficacy *indirectly* using Fourth Amendment law.

Part V.A describes the anemic programmatic efficacy review that the Supreme Court has incorporated into judicial Fourth Amendment interest balancing. Part V.B proposes a more robust programmatic efficacy review by an administrative overseer and shows how one potential overseer—the Privacy and Civil Liberties Oversight Board—is already taking some important steps in this direction. It then suggests a potential interaction between administrative efficacy review and judicial review under the Fourth Amendment.

---

324. *See* Meares, *supra* note 6, at 162-63.

325. *See id.* at 161 ("[T]he Fourth Amendment . . . calls for a reasonable balance between liberty and order, seemingly an explicit invitation to consider law enforcement effectiveness.").

A. Judicial Reluctance to Review Programmatic Efficacy

Courts routinely undertake individualized efficacy assessments under the Fourth Amendment. When a court determines whether probable cause justifies a search, it is deciding whether there is a sufficient likelihood that the search will be efficacious—that is, whether the individualized intrusion is justified as a constitutional matter.[326] Courts have been reluctant, however, to evaluate *programmatic* efficacy under the Fourth Amendment.

The Supreme Court has recognized that efficacy is a consideration relevant to balancing the interests that shape Fourth Amendment reasonableness.[327] Yet the Court has largely refrained from making efficacy a meaningful facet of its reasonableness review. Indeed, the Court has gone so far as to caution state and lower courts that efficacy review should not be *too* searching. In *Michigan Department of State Police v. Sitz*, motorists challenged the constitutionality of a highway sobriety checkpoint program under the Fourth Amendment.[328] The trial court received extensive testimony on the efficacy of the program and found that the "sobriety checkpoints were not an effective means of combating drunk driving."[329] The Supreme Court reversed the lower court's finding of constitutional unreasonableness, emphasizing that its role was not to displace the judgment of "politically accountable officials" or "[e]xperts in police science."[330]

If the Fourth Amendment requires balancing privacy and security, however, efficacy is a significant dimension of reasonableness.[331] To see why, we can turn again to the discovery of multiple-communication transactions in the section 702 program. As a result of MCTs, thousands of domestic communications unrelated to a foreign intelligence target are swept up as part of a surveillance program created to collect communications of non-U.S. persons overseas. A legal authority designed to authorize surveillance against a category of individuals largely believed to be outside the scope of the Fourth

326. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The task of [the magistrate judge] is simply to make a practical, common-sense decision whether . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.").

327. *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995).

328. 496 U.S. 444, 447 (1990).

329. Sitz v. Dep't of State Police, 429 N.W.2d 180, 183 (Mich. Ct. App. 1988) (summarizing trial court's findings), *rev'd*, 496 U.S. 444; *see also Sitz*, 496 U.S. at 448.

330. *Sitz*, 496 U.S. at 453-54. In other cases, the Court has punted on the question of efficacy by framing it as a question of least restrictive means and by rejecting such a standard for Fourth Amendment reasonableness. *See Vernonia*, 515 U.S. at 663-64; Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 629 n.9 (1989); *see also* Floyd v. City of N.Y., 959 F. Supp. 2d 540, 556 (S.D.N.Y. 2013) (declining to consider efficacy as relevant to Fourth Amendment challenge to stop-and-frisk program).

331. *See* Meares, *supra* note 6, at 161.

Amendment is being used to collect many thousands of communications of individuals with Fourth Amendment rights—disrupting the legal silos around which Fourth Amendment law organizes search and seizure power. The MCTs problem is also fundamentally a spillover problem: surveillance directed at one group of persons is sweeping up the communications of another group entirely. And it is exacerbated by a series of aggregation problems. The data are susceptible to ongoing and cumulative searches, including queries for specific U.S. persons in the section 702 datasets. In light of all of this, is upstream collection under section 702 still reasonable under the Fourth Amendment?

The FISC reviewed with care the specific rules that the government adopted to address the use and dissemination of information derived from MCTs, initially rejecting the agencies' minimization rules and ultimately approving a modified version of them.[332] But when it came to the question of programmatic efficacy, the FISC effectively punted. It noted potentially relevant considerations such as the availability of a different collection tool in the simultaneous and parallel downstream collection program.[333] Yet the court ultimately had little to go on other than the Justice Department's and NSA's assertions of a substantial security need.

One way to understand this judicial reluctance is a comparative institutional judgment that courts are not well suited to evaluate programmatic efficacy (or, at least, that they are less competent than the other branches to do so). This is an interpretive claim, though it finds support in some of the Supreme Court's own reasoning.[334] For efficacy review to be meaningful, it should be grounded in data rather than intuition.[335] Efficacy review should be relational; it should consider a particular type of collection relative to alternatives. And efficacy determinations should consider tradeoffs—that is, costs and benefits—systemically, for they may not be apparent from any one-off application.[336]

Courts are institutionally constrained in evaluating efficacy systemically and holistically. This is especially true to the extent that courts would engage in programmatic efficacy review in the context of individualized exclusionary

---

332. *See* Redacted, 2011 WL 10945618, at *11-13 (FISA Ct. Oct. 3, 2011) (rejecting the agencies' minimization rules); Redacted, 2011 WL 10947772, at *24-25 (FISA Ct. Nov. 30, 2011) (approving a modified version of the agencies' minimization rules).

333. *See* Redacted, 2011 WL 10945618, at *36-37.

334. *See Sitz*, 496 U.S. at 453-54.

335. *See* Sunstein, *supra* note 168, at 2.

336. *See* Meares, *supra* note 6, at 178-79 ("Understanding stop-and-frisk as a program reveals the true costs . . . because those who experience [stop-and-frisk]—primarily young men of color—experience it as a program and not as an individual incident.").

rule determinations and suppression motions practice.[337] Even if programmatic efficacy review were a dimension of administrative law, the capacity of courts to undertake this type of review in the first instance is limited.[338]

The answer to these institutional constraints elsewhere in the administrative state has been to move reasonableness-as-efficacy review outside of the courts, at least in the first instance. We can do the same here. We can create—or, I will argue, turn to an existing—administrative structure to undertake efficacy review of surveillance programs. This type of administrative review would provide an important complement to judicial review under the Fourth Amendment. Administrative review could enable a more systemic and data-driven assessment than courts have shown a proclivity to undertake on their own. Courts, in turn, could look to efficacy review by an independent administrative overseer in making their own reasonableness assessment under the Fourth Amendment. The challenge is to create an administrative process with some institutional remove—some independence from the operational agencies on the front lines—while preserving the agility

337. Christopher Slobogin has argued that courts should conduct a relational assessment that he terms "proportionality analysis" in the course of ordinary Fourth Amendment adjudication. Slobogin's proportionality analysis would be based on data from public opinion surveys asking individuals to rate the "intrusiveness" of government surveillance techniques. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 180-86, 206 (2007); *see also* Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1589-95 (2010) [hereinafter Slobogin, *Proportionality, Privacy*]. This proportionality assessment, Slobogin argues, should inform the court's assessment of whether a warrant or some lesser process is needed for the government to collect the information at issue. I share the concerns about institutional competence that others have raised with Slobogin's proposal. *See* Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951, 964 (2009). *But see* Slobogin, *Proportionality, Privacy*, *supra*, at 1589-94, 1599-1601 (responding to critiques).

338. In the context of regulatory cost-benefit analysis, some scholars have expressed doubts about the ability of courts to adequately review this analogous type of efficacy determination when it is made in the first instance by an agency. For recent writing in the context of financial regulation and cost-benefit analysis, see, for example, John C. Coates IV, *Cost-Benefit Analysis of Financial Regulation: Case Studies and Implications*, 124 YALE L.J. 882, 909-20 (2015), raising concerns even about judicial review of cost-benefit analysis undertaken by agencies in the first instance, and Eric A. Posner & E. Glen Weyl, *Cost-Benefit Analysis of Financial Regulations: A Response to Criticisms*, 124 YALE L.J. F. 246, 261-62 (2015), disagreeing with Coates on other grounds but sharing concerns about judicial review of administrative cost-benefit analysis of financial regulation. *But see* Catherine M. Sharkey, State Farm *"with Teeth": Heightened Judicial Review in the Absence of Executive Oversight*, 89 N.Y.U. L. REV. 1589, 1591-92 (2014) (arguing for more stringent judicial review of agency cost-benefit determinations when the analysis was conducted by an independent agency without executive oversight).

and know-how that come from situating this type of review inside the administrative state.

B. Administrative Efficacy Review

Congress or the President could mandate that the executive branch make and, to the extent possible, publish a *programmatic probable cause determination* before a surveillance program is initiated. Surveillance programs are ongoing, and technological facts and government needs can change over time. For this reason, even once a surveillance program has been initiated, programmatic probable cause determinations should be reevaluated periodically.

The programmatic probable cause determination should be grounded in the specific objectives and technological tools of the program in question, and the determination should be data-driven and relational: Does just cause exist for this surveillance program, given the systemic costs and expected benefits of the type of surveillance at issue, the safeguards in place, and the reasonable alternatives? The efficacy metrics used by the executive should be disclosed by the executive in advance of their use in evaluating specific programs.[339] A programmatic probable cause determination would require the executive branch to apply those metrics in light of the specific goals of the surveillance program, the reasons why the particular set of surveillance tools was chosen to meet those objectives, the systemic privacy concerns presented, and the myriad interacting agency policies in place to protect Fourth Amendment interests during the course of collection, access, sharing, retention, and use.[340]

1. Structuring programmatic efficacy review

Structuring this type of administrative oversight implicates considerations of institutional independence and expertise.[341] In this Subpart, I explain the

339. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 148 (recommending that the executive branch "develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs" (italics omitted)); PCLOB SEC. 215 REPORT, *supra* note 221, annex B at 217 (separate statement of Board Member Elisebeth Collins Cook) (recommending that the executive "develop metrics for assessing the efficacy and value of intelligence programs, particularly in relation to other tools and programs").

340. It might be useful to think about such an approach in conceptual cost-benefit analysis terms. John Coates has argued in the context of financial regulation that "conceptual" or "qualitative" cost-benefit analysis may be worthwhile, even in contexts where the benefits of monetized cost-benefit analysis are elusive or contestable. As Coates explains, "[Cost-benefit analysis] can function as a disciplined framework for specifying baselines and alternatives, for ensuring that (at least conceptually) both costs and benefits of a rule are considered, and for encouraging reliance on 'evidence' rather than *solely* on intuitive judgment." Coates, *supra* note 338, at 892-93.

341. In the context of congressional oversight over intelligence gathering, Anne Joseph O'Connell has framed the central design question as centralization versus redundancy.
footnote continued on next page

desirability of a centralized administrative overseer with some institutional remove from the operational agencies on the front lines, and I explore two relevant types of expertise. In the next Subpart, I explain why creating some institutional remove from the President is also desirable.

Locating efficacy review in a centralized overseer, external to the operational agencies, can help to overcome the problem of "secondary mandates."[342] Agencies charged with both a primary and a secondary mission will tend to prioritize their primary mission, particularly in circumstances when the two missions are (or appear to the agency to be) in tension.[343] This concern with administrative resistance to secondary mandates helps explain the functions of the Warrant Clause as well. Crime reduction is the primary mandate of the police, and protecting privacy interests can be viewed as a secondary mandate. A key concern underlying the warrant requirement is that the investigating officer, focused on evidence collection, will not pay sufficient heed to those secondary mandates on her own. For this reason, the warrant requirement interposes an external overseer (the magistrate judge) with a different institutional orientation.[344] So too, administrative law theorists have

---

See O'Connell, *supra* note 29, at 1657. In the context of administrative oversight, however, decentralized oversight would mean situating overseers inside the operational agencies rather than relying on an external, centralized overseer. For this reason, my discussion frames the core tradeoff here as one between (relative) independence and expertise.

342. *See* J.R. DeShazo & Jody Freeman, *Public Agencies as Lobbyists*, 105 COLUM. L. REV. 2217, 2221 (2005).

343. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75 (2008) (exploring how two agencies complied with the new statutory requirement for privacy impact assessments in connection to certain information technology systems and finding markedly different adherence to this secondary mandate); Barkow, *supra* note 29, at 275, 306-19 (arguing that the problem of dual mandates helps to explain pathologies in the Justice Department's administration of clemency, forensic science, and prison reform because each of these mandates is secondary to Justice Department's prosecutorial mission); Berman, *supra* note 29, at 75-76 (arguing that PCLOB should have "a seat at the table" when the Attorney General promulgates domestic intelligence guidelines for the FBI to help alleviate the "secondary mandates" problem); DeShazo & Freeman, *supra* note 342, at 2228-30 (arguing that Congress strengthened the Federal Energy Regulatory Commission's (FERC) compliance with its secondary mandate of environmental protection in hydropower licensing decisions by empowering other environmental resource agencies to "lobby" FERC for greater environmental protections); Sinnar, *supra* note 16, at 331 (arguing that the secondary mandates problem is especially acute where the secondary mandate is rights protection and the primary mandate is security, in part because "protection of individual rights often serves as a constraint on security agencies rather than as a secondary, affirmative mandate" (emphasis omitted)).

344. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2482 (2014) (reasoning that the warrant requirement "ensures that the inferences to support a search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often

footnote continued on next page

looked for institutional mechanisms to bolster an agency's adherence to its secondary mandates. And a key move in the recent scholarship has been to look to another agency to provide that institutional pressure point.[345]

The flipside of relative impartiality or insulation from the intelligence and law enforcement agencies is competence or expertise. In the context of surveillance technologies, technological expertise is particularly vital for effective oversight. Understanding how the collection and use technologies operate in practice is a necessary predicate to determining their appropriate scope. The administrative actors undertaking collection will be closest to those fast-changing facts on the ground.

That said, there is a second type of expertise that centralized oversight is uniquely able to provide. Centralized review enables a more synoptic expertise—that is, visibility into how overlapping and interconnected administrative policies (designed by different actors) in combination create systemic privacy risks or safeguards. Administrative law scholars have argued that this more systemic type of expertise is a distinct competency of the Office of Information and Regulatory Affairs (OIRA) relative to the individual agencies charged with rulemaking.[346] It is especially important for surveillance governance because privacy risk is cumulative. A centralized overseer can better respond to both the aggregation and the spillover problems posed by programmatic surveillance, especially where these problems arise from interdependent actors and policies spread out across the administrative state. Centralized review would be preferable, then, particularly if other institutional mechanisms existed to compensate for the more "retail-level" expertise needs.[347]

---

competitive enterprise of ferreting out crime'" (quoting Johnson v. United States, 333 U.S. 10, 14 (1948))); McDonald v. United States, 335 U.S. 451, 455-56 (1948).

345. *See, e.g.*, DeShazo & Freeman, *supra* note 342, at 2228-30; Sinnar, *supra* note 16, at 325-30.

346. *See, e.g.*, Barkow, *supra* note 171, at 30-31; Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1178-80 (2012); Michael A. Livermore & Richard L. Revesz, *Regulatory Review, Capture, and Agency Inaction*, 101 GEO. L.J. 1337, 1367-70 (2013); Cass R. Sunstein, *The Office of Information and Regulatory Affairs: Myths and Realities*, 126 HARV. L. REV. 1838, 1855-56 (2013).

347. Institutional structures internal to the agencies could contribute to programmatic probable cause review. Recent years have seen a proliferation of "privacy impact officers" and other "offices for civil rights and civil liberties" inside the agencies. Margo Schlanger has provided an important account of those institutions based on a case study of DHS's Office for Civil Rights and Civil Liberties. Schlanger analyzes the ways in which such offices, which she terms "Offices of Goodness," can intervene in and improve agency operations. *See* Schlanger, *supra* note 29, at 55, 92, 96. Schlanger further elaborates the dynamics between these internal-to-the-agency institutions and external overseers, who both benefit from the information generated by these internal institutions and contribute to their success. *See id.* at 106-11. For earlier work elaborating the role and efficacy of privacy impact officers in two agencies, see

footnote continued on next page

2. Decentering executive oversight from the President

If there is an important role for centralized oversight, then we must locate a center. Administrative law and political science theorists often situate centralized oversight inside the Executive Office of the President (EOP). A conventional move has been to couple centralized oversight with presidential oversight. This is in part because the dominant normative defense of centralized oversight has been an argument for political accountability rooted in the presidency. It is also because the prominent examples of centralized review have tended to be White House structures. In a just-published article, Samuel Rascoff builds on this literature to argue for closer presidential control over intelligence collection, through more centralized oversight inside the White House as well as more political appointees inside the intelligence agencies.[348]

Centralized oversight is not coterminous with presidential oversight, however, as leading OIRA scholars have shown.[349] The burgeoning administrative law scholarship on the interagency space further reveals agencies checking and fueling each other's work. In some contexts, it will be especially important to build in some institutional remove from the White House complex.[350] Immediate political pressures are ever-present inside the EOP, and many of its institutions are specifically designed to respond to those political and communications challenges.[351] A measure of insulation from those dynamics is valuable where public safety and security interests intersect with long-term privacy and liberty concerns.

Bamberger & Mulligan, *supra* note 343. For a discussion of inspectors general as internal overseers, see Sinnar, *supra* note 29.

348. *See* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633 (2016). Rascoff's proposals translate to the intelligence space two institutional strategies that Terry Moe has argued are available to the President to exercise greater control over the bureaucracy. *See* Terry M. Moe, *The Politicized Presidency*, *in* THE NEW DIRECTION IN AMERICAN POLITICS 235, 244-45 (John E. Chubb & Paul E. Peterson eds., 1985).

349. *See, e.g.*, Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 COLUM. L. REV. 1260, 1307-08 (2006); Livermore & Revesz, *supra* note 346, at 1347-48; *see also* Steven Croley, *White House Review of Agency Rulemaking: An Empirical Investigation*, 70 U. CHI. L. REV. 821, 873-74 (2003) (describing administrative and technocratic features of OIRA review).

350. Separation of powers considerations will affect the degree of insulation that is legally permissible. But creating a structure outside of the EOP will enable a measure of insulation from those immediate political pressures, even if the agency overseer is still subject to presidential supervision. For explorations of agency independence along a spectrum and the availability of different types of insulation mechanisms, see Barkow, *supra* note 171; and Kirti Datla & Richard L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies)*, 98 CORNELL L. REV. 769 (2013).

351. *See, e.g.*, Jon D. Michaels, *The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond*, 97 VA. L. REV. 801, 830-31 (2011).

Rascoff's argument that presidentializing intelligence-collection oversight makes for a more "rights-regarding intelligence"[352] appears grounded in a particular political moment, in the aftermath of the Snowden disclosures, when technology companies are mobilized to push back through White House channels.[353] Other examples of presidentialized intelligence, however, rooted in different political moments, have yielded significantly less rights-protective intelligence. The widely repudiated President's Surveillance Program (PSP), institutionalized by President George W. Bush and conducted pursuant to recurring presidential authorizations through a centralized process inside the White House, provides a stark illustration.[354] Thus, while the President may have an important role to play in setting national strategic direction for intelligence collection, a centralized administrative overseer can help to institutionalize rights protections with some important remove from White House pressures.

To be clear, this is not an argument against presidential supervision of the administrative state. Rather, it is an argument about how the administrative institutions that inform presidential decisionmaking should be designed. Creating a centralized administrative overseer with some insulation from the White House can help in the administration of even the most closely held presidential powers.[355] Thus, while I agree with Rascoff that current political dynamics create an important opportunity for structural surveillance reform,[356] using that momentum to enhance institutions with some remove

352. Rascoff, *supra* note 348, at 688-92.

353. *See id.* at 660-69. Rascoff recognizes that the "antisurveillance sensibilities" of these technology companies might shift over time, but he argues that presidential intelligence "will already have taken on an institutional life of its own." *Id.* at 644. But if, as Rascoff argues, an advantage of presidential intelligence is responsiveness to this emergent interest group, then the policy preferences derived through presidential intelligence might evolve with those interest group preferences. *Cf.* McNollgast, *The Political Economy of Law*, *in* 2 HANDBOOK OF LAW & ECONOMICS 1651, 1707-15 (A. Mitchell Polinsky & Steven Shavell eds., 2007) (synthesizing earlier work by the authors arguing that Congress exercises ex ante control over future agency policy outputs through administrative procedures that empower specific interests).

354. *See, e.g.*, OFFICE OF INSPECTORS GEN. OF THE DEP'T OF DEF. ET AL., REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009), http://nyti.ms/1OQNLwq. Rascoff argues that the PSP is not an instance of "presidential intelligence" as he would define the term. *See* Rascoff, *supra* note 348, at 655. Yet the PSP reveals a very different impact of presidential control on intelligence governance. The section 702 program grew out of efforts to put facets of the PSP on a more viable legal footing. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 16-20; Donohue, *supra* note 158, at 124-28.

355. *Cf.* Rachel E. Barkow & Mark Osler, *Restructuring Clemency: The Cost of Ignoring Clemency and a Plan for Renewal*, 82 U. CHI. L. REV. 1 (2015) (proposing the creation of a clemency commission to assist the President in the exercise of the pardon power).

356. *See infra* note 401.

from the White House might offer a more enduring mechanism for protecting Fourth Amendment interests.[357]

Another potential center emerges from the administrative law scholarship: the agency as a "regulator of regulators."[358] One agency's oversight of another agency's work can take different forms, from consultation requirements to vetoes.[359] Administrative design can require one administrative actor to authorize—effectively, to provide a "warrant"—for the actions of another agency. One option would be to create a new agency to serve these functions. The start-up costs of creating a new agency, however, are considerable. It can take years to effectively stand up a new administrative body. The vitality of such an agency, moreover, is contingent on factors often unknown and potentially unknowable at the agency's creation. These include "conventions" of independence that evolve over time and can be significant for the agency's on-the-ground independence.[360]

Another option would be to augment the role of the Attorney General. In the context of foreign intelligence, the Attorney General has long played the role of "regulator of regulators." Longstanding presidential directives require the Attorney General to authorize foreign intelligence activities inside the United States or against a U.S. person abroad.[361] Presidential directive also

---

357. Of course, rights protection is not the only dimension of intelligence governance, *see* Rascoff, *supra* note 348 (discussing, inter alia, strategic relations with foreign powers), and so structures institutionalizing rights should not substitute for national strategic direction, including, where appropriate, through the President. Whether those presidentialized structures and processes already exist or should be further institutionalized is a question beyond the scope of this Article but subject to a robust debate in the January 2016 issue of the *Harvard Law Review Forum*, which engages Rascoff's article.

358. Jacob E. Gersen, *Administrative Law Goes to Wall Street: The New Administrative Process*, 65 ADMIN. L. REV. 689, 701 (2013); *see also* Eric Biber, *The More the Merrier: Multiple Agencies and the Future of Administrative Law Scholarship*, 125 HARV. L. REV. F. 78, 81 (2012).

359. *See, e.g.*, Freeman & Rossi, *supra* note 346.

360. *See* Adrian Vermeule, *Conventions of Agency Independence*, 113 COLUM. L. REV. 1163, 1165-68 (2013).

361. The requirement is today contained in an executive order, *see* Exec. Order No. 12,333, § 2.5, 3 C.F.R. 200 (1981), and originated in a memorandum from President Johnson, *see* Memorandum from President Lyndon B. Johnson to the Heads of Exec. Dep'ts & Agencies (June 30, 1965), https://www.gpo.gov/fdsys/pkg/GPO-CHRG-REHNQUIST-POWELL/pdf/GPO-CHRG-REHNQUIST-POWELL-7-3-3-7.pdf. In its review of the intelligence agencies' security activities, the Church Committee emphasized the significance of Attorney General oversight and recommended that the role of the Attorney General with respect to domestic intelligence collection be strengthened. *See* SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 332-33 (1976).

requires the Attorney General to approve procedures created by the agencies constituting the intelligence community (such as the NSA) that govern collection, retention, and dissemination of foreign intelligence information concerning U.S. persons.[362]

While the Attorney General's oversight role makes historical sense, it is today problematic. The intelligence community historically conducted foreign intelligence directed overseas, and the Attorney General oversaw domestic law enforcement. As an institutional matter, then, the Office of the Attorney General was steeped in a legal tradition of constitutional, statutory, and policy constraint that looked very different from the one in which the intelligence community operated. The Attorney General was able to bring this distinct and law-informed perspective to bear on intelligence community activities inside the United States or involving U.S. persons. Yet the evolution of the Justice Department into a national security and intelligence agency, with counterterrorism as its top priority, diminishes the capacity of that office to serve as the dispassionate overseer of programmatic surveillance.[363] The Justice Department's national security mission is in considerable tension with the role of the Attorney General as a guardian of Fourth Amendment values inside the executive branch.

Instead, centralized review should be assigned to an agency specifically focused on the privacy interests underlying the Fourth Amendment—an agency with some remove from both the Justice Department and the White House.

3. The Privacy and Civil Liberties Oversight Board as a systemic regulator of efficacy

The Privacy and Civil Liberties Oversight Board (PCLOB) is an institutional actor, fairly new on the scene but potentially well positioned to evaluate programmatic probable cause. The PCLOB grew out of a recommendation by the National Commission on Terrorist Attacks upon the United States (the "9/11 Commission") for "a board within the executive branch to oversee adherence to . . . the commitment the government makes to defend our civil liberties."[364] The PCLOB was initially designed as an oversight body inside the EOP, but it confronted considerable challenges in implementing its

362. *See* Exec. Order No. 12,333, § 2.3, 46 Fed. Reg. 59,941 (Dec. 4, 1981); *see also* Schlanger, *supra* note 307, at 129-33.

363. *See* Berman, *supra* note 29, at 67.

364. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 395 (2004) (bolding omitted).

mandate.[365] White House interference with its work ultimately led to a high-profile resignation.[366] Congress, in 2007, reconstituted the PCLOB as an "independent agency within the executive branch."[367] The Board consists of a full-time chairman and four members, each appointed to a term of six years.[368] The Board's purpose is to ensure that privacy and civil liberties are "appropriately considered" in the executive branch's counterterrorism activities.[369] To this end, the Board has both an "advice and counsel" function and an "oversight" function.[370] Its "oversight" role includes review of counterterrorism operations and guidelines to ensure that privacy and civil liberties are "appropriately protect[ed]."[371] That oversight role is limited, however, to a reporting function.

Even in that limited capacity, the PCLOB has taken some important first steps toward developing a framework for programmatic efficacy review. Though its statutory mandate does not currently require it, the PCLOB, in its first two major reports, decided to consider programmatic efficacy. In its first report, on the bulk metadata collection program instituted under section 215, a majority of the Board concluded that the program did not "yield[] material counterterrorism results that could not have been achieved without [it]."[372]

---

365. In response to the 9/11 Commission Report's recommendation, the President initially created an interagency board chaired by the Deputy Attorney General. *See* Exec. Order No. 13,353, 69 Fed. Reg. 53,585 (Sept. 1, 2004). Congress then created a Privacy and Civil Liberties Oversight Board inside the Executive Office of the President. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1061, 118 Stat. 3638, 3684-88.

366. *See* Lanny Davis, *Why I Resigned from the President's Privacy and Civil Liberties Oversight Board—And Where We Go from Here*, HILL (May 18, 2007), http://thehill.com/blogs/pundits-blog/the-administration/34214-why-i-resigned-from-the-presidents-privacy-and-civil-liberties-oversight-board--and-where-we-go-from-here-; *see also* Sinnar, *supra* note 16, at 317.

367. *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, sec. 801(a), § 1061(a), 121 Stat. 266, 352 (codified at 42 U.S.C. § 2000ee(a) (2014)).

368. 42 U.S.C. § 2000ee(h)(1), (4). The four members currently serve in a part-time capacity. The statute specifies that the chairman shall be full-time and that the members shall be compensated "for each day during which that member is engaged in the actual performance of the duties of the Board." *See id.* § 2000ee(h)(1); *id.* § 2000ee(i)(1)(B). Underscoring the difficulty of creating an agency from whole cloth, it took several years from the passage of legislation creating the PCLOB to get the agency constituted. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., SEMI-ANNUAL REPORT: MARCH 2013-SEPTEMBER 2013, at 3-4 (2013).

369. 42 U.S.C. § 2000ee(c).

370. *Id.* § 2000ee(d)(1), (2).

371. *Id.* § 2000ee(d)(2)(C).

372. *See* PCLOB SEC. 215 REPORT, *supra* note 221, at 146. *But see id.* annex A at 212 (separate statement of Board Member Rachel Brand) (dissenting from Board's conclusion

footnote continued on next page

Shortly thereafter, the PCLOB reviewed the section 702 program and determined that this program *did* constitute an effective counterterrorism tool.[373] The Board was unanimous in its efficacy conclusion in the section 702 report but splintered on significant legal-policy considerations involving the program's implementation.[374] While the PCLOB's section 215 report was celebrated as an important check on the intelligence community and is believed to have helped fuel the significant changes to that legal authority that followed (first through presidential directive and ultimately in legislation),[375] the section 702 report has led some to argue that the Board is a rubber stamp for the surveillance state.[376]

Yet a close look at the PCLOB's analyses reveals a nuanced, granular, and relational assessment of programmatic efficacy, as well as a more transparent and inclusive process than otherwise would have occurred. The two reports, in combination, suggest a gradual evolution toward an administrative framework for efficacy review—one that includes both quantitative data and a qualitative assessment of how the program is advancing concrete goals and whether more privacy-protective alternatives exist.[377] The PCLOB also served as an important institutional interface between the law enforcement and intelligence agencies and the domestic public. In the course of preparing its

---

regarding the value of the section 215 program and arguing that "[i]ts usefulness may not be fully realized until we face another large-scale terrorist plot"); *id.* annex B at 217 (separate statement of Board Member Elisebeth Collins Cook) (disagreeing with the Board's efficacy conclusion but emphasizing the need for metrics to assess "the efficacy and value of intelligence programs").

373. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 104.

374. *Compare, e.g.*, *id.* annex A at 151 (separate statement of Chair David Medine and Board Member Patricia Wald) ("We do not believe that the Board[] . . . goes nearly far enough to protect U.S. persons' privacy rights when their communications are incidentally collected as a consequence of targeting a non-U.S. person located abroad under Section 702."), *with id.* annex B at 161 (separate statement of Board Members Rachel Brand and Elisebeth Collins Cook) (underscoring division within the Board on this question and the appropriate privacy safeguards).

375. *See, e.g.*, Sinnar, *supra* note 16, at 320 ("Although the PCLOB report's impact cannot be isolated from other sources of pressure to change the program, it likely further pushed the administration to agree to change course.").

376. *See, e.g.*, David Kravets, *Shocking!: Obama's Privacy Board OKs Massive NSA Surveillance*, ARS TECHNICA (July 2, 2014, 9:08 AM PDT), http://arstechnica.com/tech-policy/2014/07/shocking-obamas-privacy-board-oks-massive-nsa-surveillance (reporting that the PCLOB's section 702 report is "largely condemned by civil liberties advocates and scholars").

377. *See, e.g.*, PCLOB SEC. 215 REPORT, *supra* note 221, at 145-48 (suggesting "seven broad ways in which an intelligence-gathering tool . . . can provide value in safeguarding the nation from terrorism" and evaluating the section 215 program under each); PCLOB SEC. 702 REPORT, *supra* note 56, at 104-10 (detailing the advantages and unique capabilities of the section 702 program, as well as its specific contributions to the government's counterterrorism efforts).

first reports, the PCLOB convened a public-comment period through www.regulations.gov and held a series of public hearings with participants from the privacy advocacy community, trade associations, technology companies, and academia.[378] The Board also met with members of the intelligence community, the Justice Department, the White House, and congressional committee staff.[379] As a result of the PCLOB's work, the myriad administrative rules governing a complex and sprawling surveillance program like section 702 are not only more visible. They are also more *accessible*—that is, more intelligible to the public, the courts, Congress, and perhaps even to the executive branch itself.[380]

This is at least in part because the PCLOB is uniquely able to both obtain and meaningfully engage with a range of information from a range of agency personnel about how a surveillance program operates in practice. As an administrative overseer inside the executive branch, the PCLOB can have access to classified information, as well as deliberative-process or privileged information that a court or Congress might not be able to obtain.[381] The PCLOB is also able to engage lawyers, policymakers, technologists, and analysts inside the operational agencies to gain an understanding of legal rationales, policy considerations, and technological realities. The PCLOB is then able to test those understandings against public comment and testimony from technology companies, civil liberties groups, academics, and others in the public space. And it can conduct its review freed of barriers like Fourth Amendment standing, the limitations on facial challenges, and the Article III constraints that courts confront.[382]

As a result, the section 702 report, for example, sets out for the first time how the various pieces of the section 702 program fit together, how and when the rules from different agencies interconnect, and what the hard and open

---

378. *See* PCLOB SEC. 702 REPORT, *supra* note 56, at 2, 179.

379. *See id.* at 2.

380. Making surveillance programs more accessible also enables institutional checks on surveillance authority from outside the executive branch. *See* JACK L. GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 (2012) (describing a new separation of powers environment shaped by legal and political constraints, including from human rights organizations, the media, and the voting public); Sinnar, *supra* note 16, at 292 ("'[R]ights by disruption' . . . relies on external pressure to disrupt the assumptions or political incentives of national security officials." (emphasis omitted)).

381. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., ANNUAL FREEDOM OF INFORMATION ACT REPORT: FISCAL YEAR 2014, at 1 (2014), https://www.pclob.gov/library/FOIA-FY14-AnnualReport.pdf; *see also* E-mail from David Medine, Chairman, Privacy & Civil Liberties Oversight Bd., to author (Mar. 6, 2016) (on file with author) (indicating that one of the PCLOB's advantages as an executive branch agency is the ability to access privileged materials that might not be available to Congress or the courts).

382. *See supra* notes 51-52, 311 and accompanying text.

legal and policy questions of program design and implementation look like. This way into a surveillance program holistically, systemically, and granularly is a crucial step to any form of meaningful legal or political accountability. And yet it is exceedingly difficult, if not impossible, to imagine an actor other than a centralized administrative structure capable of obtaining and synthesizing that information from the various actors and making it both coherent and accessible. In fact, it is unlikely that any single intelligence agency had available to it this comprehensive account of the section 702 program before the PCLOB completed its review.

A programmatic probable cause requirement could institutionalize and enhance this emergent administrative oversight. Centralized review by the PCLOB could also embrace—explicitly and transparently—a hybrid legal-policy posture more easily than a court could. Reasonableness interest balancing under the Fourth Amendment involves making difficult policy tradeoffs. We cannot meaningfully implement the Fourth Amendment if its interest balancing occurs only through institutions reticent to make or openly acknowledge those inevitable policy tradeoffs. Centralized efficacy review, by an administrative overseer, could openly reclaim some of that legal-policy work for Fourth Amendment interest balancing.[383]

A more muscular PCLOB could be required to determine whether programmatic probable cause exists for new and ongoing surveillance programs on a periodic basis.[384] The PCLOB could also be authorized to

383. The interconnection between law and policy in constitutional reasonableness review explains not only why an administrative overseer is an important complement to a court like the FISC but also the value of PCLOB review as compared to other institutions of legal review inside the executive branch. Shirin Sinnar has argued that the PCLOB is a "'second-tier' legal office[] . . . unlikely to constrain national security agencies in interpreting . . . the legal scope of rights," in contrast, for example, to the OLC inside the Justice Department. *See* Sinnar, *supra* note 16, at 293, 340-41. But the OLC has built its institutional standing in part by declining to engage in hybrid legal-policy review, instead limiting its role solely to questions of law. While carving out that institutional role may enhance the OLC's power in some contexts, it makes it difficult for the OLC to undertake a type of efficacy review under the Fourth Amendment that is different from the exceedingly deferential efficacy review that the courts have been willing to undertake. For this reason, while the PCLOB is not a central actor in executive-branch legal interpretation generally, it might be a superior actor to the OLC for implementing reasonableness under the Fourth Amendment.

384. A systemic approach to risk is reflected, for example, in the creation of the Financial Stability Oversight Council, an interagency group designed to provide for more systemic financial risk oversight. One of the Council's principal tasks is to oversee the work of the individual financial regulators (like the SEC) in order to identify and address more systemic concerns. *See* 12 U.S.C. § 5330 (2014); *see also* Gersen, *supra* note 358, at 701. The Council can "provide for more stringent regulation of a financial activity" by recommending new or heightened standards and safeguards to the principal financial regulator "if the Council determines that the conduct, scope, nature, size, scale, concentration, or interconnectedness of such activity or practice could

footnote continued on next page

recommend heightened privacy safeguards that the operational agencies would then be required to adopt or otherwise respond to in writing. The scope of activities subject to this type of administrative review could be expanded beyond counterterrorism to significant surveillance programs involving the federal law enforcement, intelligence, and security agencies.[385] And a presumption of transparency and participatory process could govern the PCLOB's review.

Such an augmented role for the PCLOB would require a significant infusion of resources and close attention to other dimensions of the agency's organizational structure.[386] It also would require careful thinking about the consequences of a decision by the PCLOB declining to find programmatic probable cause. Disagreement between the PCLOB and the operational agencies might be elevated to the President, for instance; any presidential decision would then be made with the benefit of the PCLOB's written assessment of programmatic efficacy. The PCLOB's determination, even when it is not public, might also be provided to the FISC or to a criminal court presented with evidence derived from the surveillance program. Without attempting to exhaust the institutional design questions that such a proposal raises, my goal here is simply to suggest that a centralized administrative overseer could provide a type of programmatic efficacy review that Fourth Amendment reasonableness seems to call for but that courts have not shown a proclivity to meaningfully undertake.

---

create or increase" systemic financial risks. 12 U.S.C. § 5330(a). If the primary regulator rejects the Council's recommendation, it must explain its reasoning in writing. *Id.* § 5330(c)(2). The Council has been the subject of criticism and litigation, and it may be too soon to tell whether it provides a viable model for financial risk regulation. *See, e.g.*, Adam J. Levitin, *The Politics of Financial Regulation and the Regulation of Financial Politics: A Review Essay*, 127 HARV. L. REV. 1991, 2041 (2014) (book review); Victoria McGrane & Leslie Scism, *MetLife Suit Sets Up Battle over Regulation*, WALL ST. J. (Jan. 14, 2015, 12:16 AM ET), http://on.wsj.com/1u2xURE. It also differs in significant respects from the proposed structure in the text (for example, its design resembles the earlier-repudiated form of an interagency council on privacy). But the Council highlights some innovative moves in the design of systemic risk regulation using an administrative overseer. *See* Gersen, *supra* note 358, at 701.

385. *Cf.* PRG REPORT, *supra* note 221, at 35, 195 (recommending a reconfigured privacy oversight board and proposing expanding its mandate to all foreign intelligence activities, rather than only counterterrorism).

386. One set of considerations that might call for structural change, for example, is how well the PCLOB is set up to handle periods of transition in its membership. The ability to appoint an acting head of the agency when a chairman steps down and for members to continue in their positions pending the confirmation of a replacement might prove vital to the ongoing operation of the agency. So too, the part-time status of the members may need to be reexamined.

4. Distinguishing efficacy review from compliance

It is important to disentangle the centralized efficacy review proposed above from the role of "compliance" oversight that has become more institutionalized inside the executive branch.[387] Both are important instruments of surveillance governance, but they serve very different purposes. Compliance oversight is about the processes through which an agency, as a complex organization, ensures its conformance with the existing legal framework.[388] Surveillance programs today are implemented by a variety of agency personnel, including operators, technologists, and mathematicians. In a time of technological complexity and fast-paced change, compliance institutions play a significant role translating the legal rules on the page to operational realities. They also help foster greater conformity with that legal framework.[389] Compliance oversight, therefore, can help prevent damaging disconnects among legal reviewers, political leadership, and the operators and technologists on the ground.

It was just such a disconnect that led to the creation of the position of NSA's first Director of Compliance.[390] In 2009, officials at the DOJ and NSA discovered that the NSA had been operating an automated searching system that used records obtained under the section 215 metadata collection program in contravention of governing agency rules.[391] Those rules, developed administratively and approved by the FISC, had required "reasonable articulable suspicion" that an identifier used to search the section 215 datasets was "associated with" a counterterrorism target.[392] The NSA, however, had been using a system that automatically scanned for a set of identifiers (an "alert list") whenever new records were added to the agency's databases. The alert list

387. In the intelligence context, Margo Schlanger has described a thick web of organizations and institutions focused on legal compliance. *See* Schlanger, *supra* note 307, at 133-72. Schlanger argues that this focus on legal compliance "has obscured the absence of what should be an additional focus on interests, or balancing, or policy." *Id.* at 118.

388. *See generally* THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 3 (Geoffrey Parsons Miller ed., 2014) (defining compliance as "the processes by which an organization polices its own behavior to ensure that it conforms to applicable rules and regulations").

389. John DeLong, the NSA's first Director of Compliance, has described compliance as "the bringing-rules-to-life business" in a technologically complex environment. Gregory J. Millman, *Compliance in Government: Q&A with John DeLong of the NSA*, WALL ST. J.: RISK & COMPLIANCE J. (Jan. 23, 2014, 12:26 PM ET), http://blogs.wsj.com/riskandcompliance/2014/01/23/compliance-in-government-qa-with-john-delong-of-the-nsa.

390. *See* Millman, *Compliance in Government*, *supra* note 389; *see also* 50 U.S.C. § 3602 (2014).

391. *See* PCLOB SEC. 215 REPORT, *supra* note 221, at 47.

392. *Id.* at 39.

was used to scan new data collected under section 215 without individualized findings of reasonable suspicion as the agency rules required.[393] In reporting this violation to the FISC, then-NSA Director Keith Alexander told the court that "'it appears there was never a complete understanding among the key personnel' . . . 'regarding what each individual meant by the terminology used.'"[394]

Compliance oversight is designed to prevent this type of disconnect and to create structural and procedural mechanisms that hold the agency to account for program implementation. For this reason, the growth of compliance organizations inside the agencies—the role of actors like inspectors general, as well as the more recent development of compliance offices—are salutary, even if imperfect.[395] Yet because compliance is about conforming institutional behavior to existing legal rules, compliance oversight cannot compensate for inadequate program design; compliance institutions are only as effective as the legal rules that they enforce. Centralized efficacy review can help to shift some attention back to that governing legal framework.

5. Dynamic governance and judicial review

Effective surveillance governance is not linear. The relationship between centralized efficacy review and compliance should be dynamic. Compliance institutions help to achieve workable legal rules in the first instance and to shine a light on gaps between legal expectations and technological or operational realities. An effective system of governance should be able to integrate those new understandings into the design of the surveillance program itself. Recall the discovery of multiple-communication transactions in the section 702 datasets. The executive designed, and the FISC initially approved, a set of rules governing section 702 on the understanding that discrete communications would be collected. But the technological facts turned out to be very different from what the legal rulemakers (both agency overseers and the FISC) initially understood them to be. Compliance oversight is designed to reveal this type of disconnect.

The discovery of multiple-communication transactions, in turn, raises this central question: Is the program still *reasonable* under the Fourth Amendment? Under the framework proposed above, the PCLOB would be required to

393. *Id.* at 47.

394. *Id.* at 48 (quoting Declaration of Lieutenant General Keith B. Alexander at 18, *In re* Prod. of Intangible Things, No. BR-13, 2009 WL 9150913 (FISA Ct. Mar. 2, 2009)). Schlanger provides a detailed account of the development of compliance institutions inside the intelligence domain in response to the Church Committee's work and the rejuvenated focus on compliance by policymakers following the 2009 incident at the NSA. *See* Schlanger, *supra* note 307, at 120-40.

395. *See* Sinnar, *supra* note 16, at 356; Sinnar, *supra* note 29, at 1031-32.

review the program's efficacy at a simultaneously more granular and more holistic level than either courts or Congress have been willing to do. This type of centralized administrative review does not ensure any particular outcome. But it offers a more robust and nuanced mechanism for efficacy review than judicial review under the Fourth Amendment.

The PCLOB's determination could in turn be reviewable by a court under the Fourth Amendment. As discussed earlier, courts have recognized programmatic efficacy as a component of Fourth Amendment reasonableness, but they have refrained from meaningfully evaluating it. Courts might be more amenable to supervising programmatic efficacy indirectly by asking whether an impartial administrative overseer has established programmatic probable cause. This type of reasonableness review under the Fourth Amendment also could enable courts to encourage, if not entrench, more systemic extrajudicial oversight.

This relationship between constitutional rights and administration is not new. Gillian Metzger describes how the now-famous *Miranda* warnings are based on federal administrative practice in place at the time of the Court's decision in *Miranda*.[396] In the Fourth Amendment context, the courts of appeals' consideration of the legality of warrantless foreign intelligence surveillance prior to the enactment of FISA effectively converted the practice of Attorney General authorizations into a Fourth Amendment requirement. What originated as a governance mechanism inside the executive branch became a part of pre-FISA Fourth Amendment doctrine.[397] Rather than judicial "road mapping,"[398] these examples show *executive* road mapping for courts. In this sense, administrative governance strategies can become—formally, not just functionally—the content of legal rights.

C. Designers and Politics

If we need to reform the structures and processes of surveillance governance, to whom should we address calls for reform? The most far-reaching reforms would require congressional action. Congress could augment the authorities, structure, and resources of the PCLOB to play a more muscular role in surveillance governance. And it could amend or enact new framework legislation to require programmatic probable cause review. This is a very

396. Metzger, *supra* note 187, at 507-08.

397. *See* United States v. Bin Laden, 126 F. Supp. 2d 264, 279-80 (S.D.N.Y. 2000) (describing this pre-FISA precedent), *aff'd on other grounds sub. nom. In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93 (2d Cir. 2008).

398. *See* Erik Luna, *Constitutional Road Maps*, 90 J. CRIM. L. & CRIMINOLOGY 1125, 1128 (2000) (describing and evaluating a judicial approach, which he terms "constitutional road map[ping]," where the Supreme Court strikes down the law in question but suggests a more viable alternative).

different role for Congress than a rule of lenity regime. Rather than looking to Congress to resolve rule-based ambiguity at every turn, Congress can play an important role in authorizing surveillance and setting up the structures and processes through which surveillance governance unfolds. To be sure, our age of polarization and gridlock makes congressional action of any sort a challenge.[399] The political economy of crime and security further impedes congressional action.[400] At the same time, in the aftermath of the Snowden disclosures, we might be at an auspicious moment for at least some types of structural surveillance reform.[401]

Even if the current political climate is insufficient to generate congressional action, it already has stimulated and is likely to stimulate more institutional reform through presidential administration.[402] Presidents have substantial incentives to adopt mechanisms that create or sustain their credibility, particularly in moments when that credibility is most heatedly on the line. Presidents are motivated to "self-bind" because these measures are

399. *See, e.g.*, Jody Freeman & David B. Spence, *Old Statutes, New Problems*, 163 U. PA. L. REV. 1, 2 (2014); *see also* Richard H. Pildes, *Why the Center Does Not Hold: The Causes of Hyperpolarized Democracy in America*, 99 CALIF. L. REV. 273, 275, 330-31 (2011).

400. *See, e.g.*, Murphy, *supra* note 12, at 503-07; William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 525-29 (2001).

401. Unlike the conventional framing of the politics of crime and security, contemporary surveillance practices implicate a powerful, emergent interest group—communications and technology companies. *See* Rascoff, *supra* note 348, at 660-69. The implications of the Snowden disclosures for these companies appear significant, and these companies are coalescing into an engaged voice in the politics of surveillance. *See, e.g.*, Tom Hamburger & Matea Gold, *Google, Once Disdainful of Lobbying, Now a Master of Washington Influence*, WASH. POST (Apr. 12, 2014), http://wpo.st/s4HY1; David E. Sanger & Steve Lohr, *Call for Limits on Web Data of Customers*, N.Y. TIMES (May 1, 2014), http://nyti.ms/1iOzF2s; Edward Wyatt & Claire Cain Miller, *Tech Giants Issue Call for Limits on Government Surveillance of Users*, N.Y. TIMES (Dec. 9, 2013), http://nyti.ms/1gRjYEu. To be sure, there remain strong corporate interests on both sides of surveillance policy, and powerful sectors of the industry have much to gain from the increased use of data mining and other surveillance-related technologies. More theoretical and empirical work is needed to show how interest group theory applies in this emergent political space. The changed political dynamics, moreover, implicate only some of the executive's surveillance practices.

402. *See* Press Release, Office of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (adopting institutional and substantive requirements for signals intelligence collection). For a close exploration of Presidential Policy Directive (PPD) 28 and an argument that it marks an emergent model of presidential control over intelligence, see Rascoff, *supra* note 348, at 669-74. For arguments challenging the significance or novelty of the processes included in PPD 28, see Carrie Cordero, *A Response to Professor Samuel Rascoff's* Presidential Intelligence, 129 HARV. L. REV. F. 104 (2016); and Daniel Severson, Note, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change*, 56 HARV. INT'L L.J. 465 (2015).

fundamentally enabling[403]: constructing a more solid foundation for programmatic surveillance, in the long run, would likely make it more durable. A programmatic probable cause determination from the PCLOB—at least with respect to counterterrorism, which is itself a highly elastic concept[404]—could be instituted through an executive order and amplified through agency practice. Even if presidential action drives institutional innovation in the first instance, it might ultimately bring congressional engagement.[405]

As detailed above, courts also entrench executive design. Courts could calibrate their deference on questions of programmatic efficacy to a more robust and participatory efficacy review by an administrative overseer. And courts could look to systemic administrative safeguards to find any one-off instance of surveillance programmatically reasonable under the Fourth Amendment.

The gears of Fourth Amendment law and administration interconnect. Administrative governance works through, is shaped by, and simultaneously reshapes rights doctrine. Surveillance governance invites careful study of that interlocking design.

Conclusion: Administrative Methods for Constitutional Governance

The Fourth Amendment today unfolds through the agencies that design and implement surveillance programs. Administrative law theory has long addressed the organization of administrative power. In an age of programmatic surveillance, administrative law can help to crystalize the defining Fourth Amendment problems and can suggest doctrinal, institutional, and organizational paths to address them.

---

403. *See* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 133 (2010); *see also* Trevor W. Morrison, *Libya, "Hostilities," the Office of Legal Counsel, and the Process of Executive Branch Legal Interpretation*, 124 HARV. L. REV. F. 62, 63-64 (2011); Richard H. Pildes, *Law and the President*, 125 HARV. L. REV. 1381, 1388, 1407-08 (2012) (book review). Within the bureaucracy, as well, Elizabeth Magill has identified the practice of agency "self-regulation"—ways in which agencies will voluntarily limit their own discretion—for example, by promulgating enforcement guidelines or procedures beyond those required by law. *See* Elizabeth Magill, *Foreword: Agency Self-Regulation*, 77 GEO. WASH. L. REV. 859, 863 (2009).

404. *See* Mariano-Florentino Cuellar, *"Securing" the Nation: Law, Politics, and Organization at the Federal Security Agency, 1939-1953*, 76 U. CHI. L. REV. 587, 678-79 (2009) (discussing the constructed and instrumental meaning of the term "security" as used by political actors).

405. And even partial reform directed only at some types of surveillance could create precedent relevant to other surveillance programs.

Modern administrative law emerged in the academy as a study of federal regulatory agencies engaged in domestic policy-setting through rulemaking and adjudication subject to judicial review under the APA. Increasingly, administrative law theory has turned its gaze outward. It has become a body of methods—a methodology—for understanding and evaluating the role of administration in national governance.

This Article has conceptualized that project along three dimensions: administrative law as an analogy for constitutional law, administrative law as subconstitutional doctrines and framework legislation governing judicial review of agency action, and administrative law as agency (and interagency) design. Each of these, of course, is a well-trodden approach in the administrative law scholarship. But it is fruitful to consider them collectively, as a dynamic and interactive body of methods for constitutional governance.

Understanding administrative law in this way opens opportunities and new challenges for the legal study of administration. It embraces the possibility of using administration to achieve systemic governance, often illusive through the mechanism of individual-rights-based adjudication alone.[406] It suggests that the core rights questions implicated by the administrative state need to be broadened beyond administrative law's traditional focus on due process. And it raises difficult questions about the generalizability of agency design principles across policy domains. Like any body of methods, administrative law has its limitations, and those limitations warrant deeper investigation. As a way to understand, evaluate, and seek to improve the work of agencies in constitutional governance, however, administrative law's methods might prove indispensable.

406. *See, e.g.*, Metzger, *supra* note 14, at 1840 (exploring systemic administration as the "linchpin" of a constitutional duty to supervise).