

2011

Designing Surveillance Law

Patricia L. Bellia

Notre Dame Law School, patricia.l.bellia.2@nd.edu

Follow this and additional works at: https://scholarship.law.nd.edu/law_faculty_scholarship



Part of the [Law Commons](#)

Recommended Citation

Patricia L. Bellia, *Designing Surveillance Law*, 43 Ariz. St. L. J. 293 (2011).

Available at: https://scholarship.law.nd.edu/law_faculty_scholarship/1169

This Article is brought to you for free and open access by the Publications at NDLScholarship. It has been accepted for inclusion in Journal Articles by an authorized administrator of NDLScholarship. For more information, please contact lawdr@nd.edu.

DESIGNING SURVEILLANCE LAW

Patricia L. Bellia*

TABLE OF CONTENTS

I. INSTITUTIONAL PATTERNS IN COMMUNICATIONS SURVEILLANCE LAW	298
A. <i>The Communications Surveillance Law Landscape</i>	299
B. <i>Surveillance Law Patterns</i>	304
1. Executive Rule-Selection	304
2. Legislative Rule-Selection	305
a. <i>Reactive statutes</i>	305
b. <i>Proactive statutes</i>	309
C. <i>Understanding the Judicial Landscape</i>	315
1. Executive Rule-Selection	317
2. Legislative Rule-Selection	319
a. <i>Reactive statutes</i>	319
b. <i>Proactive Statutes</i>	319
3. Summary	326
II. FROM FIRST-ORDER TO SECOND-ORDER QUESTIONS IN SURVEILLANCE LAW	327
A. <i>Comparative Institutional Competence</i>	328
1. Executive Rule-Selection	329
2. Legislative Rule-Selection	330
3. Summary	332
B. <i>Second-Order Design Questions</i>	333
1. First-Order Preferences versus Second-Order Design Choices	333

* Professor of Law and Notre Dame Presidential Fellow, Notre Dame Law School. I thank Nicole Garnett, Orin Kerr, Liz Magill, John Nagle, Rich Schragger, Peter Swire, participants at faculty workshops at the George Washington University School of Law, the University of Virginia School of Law, and the University of Pennsylvania School of Law, and students in Michigan Law School's Intellectual Property seminar for helpful comments. George Jiang provided excellent research assistance.

I am honored to have been invited to contribute to this symposium celebrating Justice O'Connor's 80th birthday. Justice O'Connor's focus on *institutional* questions throughout her tenure on the Court has influenced legal scholarship profoundly. This Essay embraces this focus by exploring institutional questions in an area about which the Court has had relatively little to say in recent years—communications surveillance law.

2. Constitutional Constraints.....	335
C. <i>The Impact of Design Choices</i>	335
III. IMPROVING DESIGN CHOICES IN COMMUNICATIONS	
SURVEILLANCE LAW	338
A. <i>Theory: Shifting Stakes and Costs</i>	339
B. <i>Application: Executive Rule-Selection and Proactive Statutes</i>	344
1. Judicial Decisions on Executive Rule-Selection.....	344
2. Proactive Statutes	345
a. <i>Crisis Response Statutes</i>	345
b. <i>Modernizing Statutes</i>	346
IV. CONCLUSION.....	347

INTRODUCTION

By all indications, communications surveillance¹ is an increasingly important weapon in government efforts to detect and thwart criminal and terrorist activities. Between 2000 and 2009, government surveillance applications under the principal statute regulating surveillance in criminal investigations, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III” or the “Wiretap Act”),² nearly doubled.³ Applications under the statute regulating surveillance in foreign intelligence

1. I use the term “communications surveillance” rather than the more common term “electronic surveillance” to capture technically different but functionally similar techniques for acquiring the content of communications and related information. The term “electronic surveillance” typically refers to the use of an electronic or mechanical device to acquire in real-time wire, oral, or electronic communications and related source and destination information. The prevalence of stored communications makes it possible for officials to retrieve communications without using any device at all, but rather by compelling production of communications and related transactional information from the third party with whom the communications are stored. I use the term “communications surveillance” to capture this practice as well as the more traditional device-based techniques. The term thus sweeps in some activities that others refer to as “transaction surveillance.” See, e.g., Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 140 (2005); Christopher Slobogin, *Technology-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 387–88 (1997).

2. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 211, 214 (codified as amended at 18 U.S.C. §§ 2510–22 (2006 & Supp. III 2009)).

3. See ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 2009 WIRETAP REPORT tbl. 7, available at <http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table7.pdf>.

investigations, the Foreign Intelligence Surveillance Act of 1978 (“FISA”),⁴ doubled between 2000 and 2008 before dropping in 2009 to a level 36% above the 2000 totals.⁵ The available statistics, moreover, dramatically undercount surveillance activities, for they do not include data on communications surveillance activities conducted under statutes requiring no reporting⁶ or activities undertaken without judicial authorization.⁷

Against this backdrop, questions of how to reconcile privacy and law enforcement interests—and, more specifically, what limits the law should impose on executive discretion—take on paramount importance. These questions have institutional as well as substantive dimensions. That is, the issue is not simply what the limits on communications surveillance should be, but who should set them—courts through application of the Fourth Amendment or legislatures through statutes and the oversight process?

For most scholars, the question of who should regulate communications surveillance activities has a straightforward answer: the task is one for the courts applying the Constitution. Because constitutionally-based regulation of communications surveillance tactics has been relatively limited since the seminal case of *Katz v. United States*⁸ in 1967, such scholars view the surveillance law landscape as one reflecting judicial abdication: courts have largely failed at reining in executive discretion and must play a more active role.⁹ For a handful of other scholars, in contrast, the limited

4. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–85c (2006 & Supp. III 2009)).

5. Letter from John Ashcroft, Attorney General, U.S. Dep’t of Justice, to L. Ralph Mechem, Director, Administrative Office of United States Courts (Apr. 27, 2001), *available at* <http://www.usdoj.gov/oipr/readingroom/2000fisa-ltr.pdf>; Letter from Ronald Weich, Office of Legislative Affairs, to James C. Duff, Director, Administrative Office of United States Courts (Apr. 30, 2010), *available at* http://www.justice.gov/nsd/foia/reading_room/2009fisa-ltr.pdf. Until the report on calendar year 2009, the Department of Justice did not differentiate between applications for electronic surveillance orders and applications for physical search orders. The figure in the text assumes that the relative proportions of physical search and electronic surveillance orders remained roughly the same between 2000 and 2009.

6. Examples include the collection of stored e-mail under the Stored Communications Act, *see infra* notes 26–29, and the collection of information on the location of a suspect’s cell phone, *see infra* notes 37–40.

7. The National Security Agency’s “terrorist surveillance program” between 2001 and 2007 offers one example. *See infra* note 52 and accompanying text.

8. 389 U.S. 347 (1967).

9. *See, e.g.,* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 9 (2007); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004) [hereinafter Freiwald, *Online Surveillance*]; Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What Katz Is Made Of?*, 41 U.C. DAVIS L. REV. 781 (2008); Susan Herman, *The USA Patriot Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67 (2006); Tracey Maclin, *Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J.

constitutionally-based regulation of surveillance tactics is not a cause for concern. Such scholars, notably Professor Orin Kerr, have argued for legislative supremacy in surveillance law on the ground that courts lack the expertise to evaluate rapidly evolving technologies.¹⁰ Even a majority of the Supreme Court recently professed (or, some might say, feigned) a concern about its ability to tackle questions about the privacy of modern communications technologies.¹¹

Explicitly or implicitly, discussions about the relative roles of courts and the legislature in policing surveillance tactics rest on premises about the comparative competence of those institutions to limit executive discretion. On one view, courts are more likely to set the right rules than legislatures are, and courts must treat executive and legislative choices far more skeptically if they are to fulfill the role that the Constitution assigns to them.¹² On another view, courts should take a hands-off approach to Fourth Amendment questions involving new surveillance techniques, thereby leaving space for congressional regulation.¹³

These inquiries into institutional competence add an important perspective to the study of communications surveillance law. They prompt us to evaluate how well courts and Congress have protected evolving communications technologies in the past, and to ask how we can expect these institutions to handle such issues in the future. This Essay seeks to deepen the institutional perspective in two ways. The first is to clarify the roles that courts and Congress have played in regulating communications surveillance techniques. For judicial abdication scholars and legislative supremacy scholars alike, the role that courts have (or have not) played in generating communications surveillance rules provides a jumping-off point for normative claims about courts' competence to generate such rules in the future.

51 (2002); Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1551 (2010); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1296 (2004).

10. See, e.g., Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); see also Jonathan F. Mitchell, *Legislating Clear-Statement Regimes in National-Security Law*, 43 GA. L. REV. 1059 (2009); Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477, 505–06, 512, 528–29 (2007).

11. *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629–30 (2010). *But see id.* at 2635 (Scalia, J., concurring in part and concurring in the judgment) (criticizing majority's position as "unnecessary" and "self-defeating").

12. See, e.g., Herman, *supra* note 9, at 118–32; Simmons, *supra* note 9, at 1357; Slobogin, *Transaction Surveillance by the Government*, *supra* note 1, at 167–82, 189.

13. See Kerr, *supra* note 10, at 857–87.

The second goal is to bring questions of institutional *design* in surveillance law to the forefront of the analysis. Discussions of the comparative competence of courts and Congress to make surveillance law rules tend to ask whether courts or legislatures should set the constraints on executive discretion, without taking account of the institutional context for implementing these constraints. Here, it is useful to distinguish between what we might call “first-order” policy preferences for our surveillance system—questions about what kinds of communications investigators can gather, for what purpose, and during what time frame—from what we might call the “second-order” design choices for implementing or enforcing those preferences. To take one example, assume a preference that surveillance of communications in a criminal case should involve only the collection of communications concerning criminal activity. Apart from the question whether it should be up to a court or Congress to set this rule, there remain questions about who should enforce it and through what mechanisms: The executive, through its own self-restraint? Courts, through suppression motions? Courts, through civil actions against those who violate the rule? Congress, through a system of oversight? Or a combination of these decision-makers and mechanisms?

In other words, it is not enough simply to ask which decision-maker is best suited to arrive at the first-order policy preferences. Without a framework for considering second-order design choices available to implement those preferences, we run the risk that our surveillance law regime will not match first-order policy preferences—or, worse, that the surveillance law regime will itself constrain the courts or Congress from evaluating and adjusting the rules the regime reflects. This Essay thus seeks to bring second-order design questions to the forefront of the surveillance law debate and to provide a framework for considering these questions.

The Essay proceeds as follows. Part I explores the relative roles that courts and Congress have played in generating communications surveillance rules. After defining the relevant landscape, this Part identifies certain institutional patterns that give rise to surveillance law challenges and analyzes judicial decisions in light of those patterns. Part II turns to second-order design questions. It begins by exploring the institutional competence arguments and showing how viewing judicial or legislative decisions in isolation rather than in sequence can oversimplify those arguments by failing to account for how design choices affect the ability of legislatures and courts to evaluate and adjust surveillance law rules. It then attempts to disentangle second-order design choices from first-order policy preferences and to show how the Constitution does and does not constrain those choices.

Part III identifies three types of design features that are likely to affect institutional decision-making: (1) features that alter the participants' *stake* in institutional processes; (2) features that generate and limit *information* available to decision-makers and others; and (3) features that affect institutional barriers to (and other constraints on) *participation* in institutional processes. It then explores how attention to these features might help to close the gap between the communications surveillance regime that exists and a regime that would match first-order preferences (however generated).

I. INSTITUTIONAL PATTERNS IN COMMUNICATIONS SURVEILLANCE LAW

Scholars who disagree about the proper roles of courts and Congress in checking executive discretion nevertheless agree about one descriptive point: there is surprisingly little judicial constitutionally-based regulation of surveillance tactics. The area is dominated by statutes, and with a few very recent exceptions, most of the statutes have not been subject to serious constitutional challenge in the post-*Katz* era.¹⁴ Although scholars agree that judicial intervention is lacking, they draw different conclusions from its absence. For judicial abdication scholars, the lack of constitutionally-based regulation signals a need for more aggressive judicial intervention. For legislative supremacy scholars, it signals that courts are, as they should, deferring to superior legislative expertise.

Because descriptive claims about past judicial regulation of communications surveillance fuel normative claims about how courts should behave, I explore the descriptive claims here. I first identify the universe of relevant statutes and key cases. I then introduce certain institutional patterns in which constitutional questions about the use of surveillance tactics arise. These patterns, I argue, permit a more nuanced

14. Exceptions include the Sixth Circuit panel opinion in *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), which was vacated by the Sixth Circuit sitting en banc, 532 F.3d 521 (6th Cir. 2008) (en banc); the recent Sixth Circuit panel opinion in the criminal phase of the *Warshak* case, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); the Ninth Circuit opinion in *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), which was ultimately reversed in relevant part by the Supreme Court, *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629–30 (2010); and a handful of recent opinions involving the use of technology to track a target's location, see *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010); *In re Application of the United States*, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010) (Smith, Mag. J.); *In re Application of the United States*, 736 F. Supp. 2d 578 (E.D.N.Y. Aug. 27, 2010) (Orenstein, Mag. J.). A district court judge apparently reversed Judge Orenstein's August 2010 opinion, but Judge Orenstein ruled the same way in a more recent case. See *In re Application of the United States*, 2010 WL 5437209 (E.D.N.Y. Dec. 23, 2010) (Orenstein, Mag. J.).

evaluation of the relative roles of courts and legislatures in setting surveillance law rules.

Two caveats are in order at the outset. First, I focus on *government* acquisition of communications and related data and leave aside the privacy concerns raised by the collection and transfer of data by private parties. The latter topic involves distinct concerns and thus deserves more extensive treatment than this Essay can provide. Second, to the extent that my analysis teases certain surveillance law patterns out of executive, legislative, and judicial action in this area, it is vulnerable to the charge that we lack a sufficient number of episodes to generalize about how institutions interact. My goal, however, is to provide a useful lens for viewing the surveillance law landscape, not to provide a complete or definitive account of institutional interactions in this area.

A. *The Communications Surveillance Law Landscape*

The Supreme Court wrestled with the Fourth Amendment's application to communications surveillance activities as early as 1928, holding in *Olmstead v. United States* that a wiretap not effected through a trespass onto private property did not violate the Fourth Amendment.¹⁵ In 1967, the Court decided two cases that would shape the constitutional and statutory frameworks for wiretapping and eavesdropping activities. In *Berger v. New York*, the Court concluded that using an electronic listening device to capture conversations in an office was a "search" under the Fourth Amendment.¹⁶ The Court further held that the New York statute authorizing courts to grant surveillance orders was constitutionally deficient.¹⁷ The next term, in *Katz v. United States*, the Court held that the use of an electronic listening device to capture a conversation is a search, even when the placement of the device (in this case, in a telephone booth) does not involve a trespass into a private area.¹⁸ The *Katz* Court thus overruled *Olmstead* and held that the test for a search is whether investigators invade the "privacy upon which [a target] justifiably relie[d]."¹⁹ As refined in Justice Harlan's concurrence²⁰ and in subsequent cases, the test for whether an investigative

15. 277 U.S. 438, 466 (1928).

16. 388 U.S. 41, 51 (1967).

17. *Id.* at 54–60.

18. 389 U.S. 347, 353 (1967).

19. *Id.*

20. *Id.* at 361 (Harlan, J., concurring).

technique constitutes a “search” for purposes of the Fourth Amendment is whether the technique invades a reasonable expectation of privacy.²¹

In the wake of *Berger* and *Katz*, Congress adopted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,²² known as Title III or the Wiretap Act. The statute generally prohibits the “intentional intercept[ion]” of communications, but sets forth procedures under which investigators can seek a court order authorizing surveillance.²³

Although the Wiretap Act strictly regulates the interception of communications, other forms of communications surveillance are not regulated as strictly. More specifically, the Wiretap Act has been understood to govern only the acquisition *in transmission* of the *contents* of communications in *criminal* investigations. Exploring each area outside of the Wiretap Act’s coverage provides a good introduction to the rest of the communications surveillance law landscape.

Transmission vs. Storage. The Wiretap Act governs the “intercept[ion]” of communications, a term defined as the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”²⁴ Although this definition does not specify that an “interception” occurs only when a communication is seized contemporaneously with its transmission, a number of courts have so held.²⁵ A separate statutory framework, adopted as part of the Electronic Communications Privacy Act of 1986 (“ECPA”)²⁶ and commonly known as the Stored Communications Act (“SCA”), regulates the privacy of stored communications. In addition to barring unauthorized acquisition of such communications, the statute authorizes government officials to compel service providers to disclose the contents of a subscriber’s communications if certain requirements are met. In some cases—when the communications in question are “in electronic storage” with the provider of an electronic communication service for 180 days or less—investigators must obtain a warrant before compelling production of the communications.²⁷ As I will

21. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

22. Pub. L. No. 90-351, tit. III, 82 Stat. 211, 214 (codified as amended at 18 U.S.C. §§ 2510–22 (2006 & Supp. III 2009)).

23. See I JAMES G. CARR & PATRICIA L. BELLIA, *THE LAW OF ELECTRONIC SURVEILLANCE* §§ 1:10–15 (2010); Patricia L. Bellia, *Surveillance Law Through Cyberlaw’s Lens*, 72 GEO. WASH. L. REV. 1375, 1490 (2004).

24. 18 U.S.C. § 2510(4) (2006).

25. See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113–14 (3d Cir. 2003); *United States v. Steiger*, 318 F.3d 1039, 1048–49 (11th Cir. 2003); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994).

26. Pub. L. No. 99-508, §§ 201–02, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–09, 2711–12 (2006 & Supp. III 2009)).

27. 18 U.S.C. § 2703(a) (2006).

discuss below, it is unclear precisely what communications qualify as communications “in electronic storage;” officials can compel production of communications not in electronic storage on far lower standards, including by obtaining a court order that falls short of the requirements for a warrant.²⁸ Especially for electronic communications, one could argue that the prospective acquisition of communications during transmission (under the Wiretap Act) and the retrospective acquisition of past communications (under the SCA) will yield precisely the same result. The SCA does not proceed from that premise, however, and only recently have courts begun to grapple with the statute’s constitutionality.²⁹

Noncontent Information. The Wiretap Act governs only the interception of the *contents* of a communication, defined as any information “concerning the substance, purport, or meaning of that communication.”³⁰ What we might call communications “attributes”³¹—such as information about the phone number associated with an incoming or outgoing call or about the source or destination of an electronic communication—are typically outside of this statutory definition. The divergent treatment between communications contents and attributes arises in part from the Supreme Court’s decision in *Smith v. Maryland*.³² In that case, the Supreme Court held that the installation of a “pen register”—understood at the time to mean a device that detects the numbers dialed in an outgoing phone call—was not a “search” under the Fourth Amendment, and therefore did not require a warrant.³³ When Congress adopted ECPA, it added statutory requirements for the installation of pen registers as well as “trap-and-trace devices” (i.e., devices used to detect the number of an incoming call). As amended, the provisions regulate devices that detect the “dialing, routing, addressing, and signaling information” associated with incoming or outgoing wire and electronic communications.³⁴ The provisions do not require a warrant; rather, investigators can obtain a court order authorizing the installation of a pen register or a trap-and-trace device based upon a

28. See *infra* notes 115–25 and accompanying text.

29. Compare *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), and *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated on reh’g en banc*, 532 F.3d 521 (6th Cir. 2008), with *Rehberg v. Paulk*, 598 F.3d 1268, 1282 (11th Cir. 2010), and *In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail*, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009).

30. 18 U.S.C. § 2510(8).

31. See Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996) (defining term).

32. 442 U.S. 735 (1979).

33. *Id.* at 740.

34. 18 U.S.C. § 3127(3)–(4).

showing that the information sought “is relevant to an ongoing criminal investigation.”³⁵ Similarly, when investigators seek not to acquire communications attributes prospectively, but rather to collect such information retrospectively from a service provider, the SCA permits investigators to compel disclosure of the information without a warrant and on a standard of relevance to an ongoing investigation.³⁶

Another category of ostensibly “noncontent” information raises a distinct set of statutory (and perhaps constitutional) concerns—cell-site location information (“CSLI”). In theory, information on the location of cell towers “hit” by a suspect’s cell phone is “signaling” information about the origin of a communication, and thus would fall within the scope of the pen/trap statute.³⁷ A separate federal statute, the Communications Assistance for Law Enforcement Act (“CALEA”), however, precludes investigators from using the pen/trap statute as the sole basis for acquiring information “that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).”³⁸ Because CSLI can be “triangulated” to produce information on the cell phone’s location—and thus the target’s location—CALEA bars the use of the pen/trap statute in this context. As I discuss later, precisely what statutes investigators must use to gather (or compel a service provider to produce) such “cell-site location information” (“CSLI”) has been a matter of dispute for several years.³⁹ Moreover, citing changes in technology that increase the precision with which CSLI will identify a subscriber’s location, two courts have recently held that apart from any questions of statutory interpretation, the Fourth Amendment itself requires investigators seeking CSLI to obtain a warrant.⁴⁰

35. *Id.* § 3122(b)(2).

36. More specifically, investigators can compel disclosure of records or other information pertaining to a subscriber through a warrant or a court order issued under § 2703(d) of the SCA. *See* 18 U.S.C. § 2703(c)(1)(A), (B) (2006 & Supp. III 2009). An order under section 2703(d) requires a showing of “specific and articulable facts showing that there are reasonable grounds to believe that” the information sought is “relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d) (2006). For certain categories of noncontent information, only a subpoena is required. *See id.* § 2703(c)(2).

37. *See* 18 U.S.C. § 3127(3) (2006).

38. 47 U.S.C. § 1002(a)(2)(B) (2006).

39. *See infra* notes 163–70 and accompanying text.

40. *See In re Application of the United States*, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010) (Smith, Mag. J.); *In re Application of the United States*, 736 F. Supp. 2d 578 (E.D.N.Y. Aug. 27, 2010) (Orenstein, Mag. J.); *see also In re Application of the United States*, 2010 WL 5437209 (E.D.N.Y. Dec. 23, 2010) (Orenstein, Mag. J.) (adhering to logic of August 2010 case despite its apparent reversal).

Foreign Intelligence Investigations. The final area of the communications surveillance law landscape concerns the authorities under which investigators can acquire information for foreign intelligence purposes, rather than for criminal investigations. In *Katz v. United States*, the Supreme Court declined to address whether the Fourth Amendment applies to national security investigations in the same way that it applies to criminal investigations, observing that “[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is not presented by this case.”⁴¹ Five years later, however, the Court had to confront the propriety of warrantless national security surveillance directly. In *United States v. United States District Court for the Eastern District of Michigan* (commonly known as the *Keith* case),⁴² the Supreme Court held that the Fourth Amendment barred the government from conducting warrantless electronic surveillance to safeguard national security, at least when the target was a *domestic* group lacking any connection to a foreign power.⁴³ The Court left open whether warrantless surveillance could proceed in a situation involving a *foreign* threat to national security.⁴⁴ The Court also noted that in national security cases, standards different from those governing conventional search warrants might satisfy the Fourth Amendment.⁴⁵

In 1978, Congress addressed some of the issues the *Keith* Court left open by passing the Foreign Intelligence Surveillance Act (“FISA”).⁴⁶ FISA requires government officials who wish to use electronic surveillance to gather “foreign intelligence information” regarding a foreign power or an agent thereof to present a request to a special court, the Foreign Intelligence Surveillance Court (“FISC”). As will become clear, FISA’s procedures, while robust, differ from the Wiretap Act’s procedures in important respects.⁴⁷

41. 389 U.S. 347, 358 n.23 (1967); *see also id.* at 362–63 (White, J., concurring) (stating that warrant requirement should not apply if the executive branch has authorized national security surveillance as reasonable); *id.* at 359 (Douglas, J., concurring) (arguing that warrant requirement should apply).

42. The case is so known for the name of the district court judge against whom the government sought a writ of mandamus, Damon J. Keith.

43. 407 U.S. 297, 320 (1972).

44. *Id.* at 308 (observing that case required “no judgment on the scope of the President’s surveillance power with respect to the activities of foreign powers”).

45. *Id.* at 322.

46. 50 U.S.C. §§ 1801–12 (2006 & Supp. III 2009).

47. *See infra* notes 69–71 and accompanying text; *In re Sealed Case*, 310 F.3d 717, 738 (Foreign Intel. Surv. Ct. Rev. 2002); Patricia L. Bellia, *The “Lone Wolf” Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 441–42 (2005).

B. *Surveillance Law Patterns*

With this sketch of the surveillance law landscape in place, it becomes possible to identify certain institutional patterns that give rise to constitutional questions about surveillance tactics. To be clear, my argument is not that all communications surveillance law emerges from the patterns I identify, nor that surveillance statutes cannot straddle multiple categories. In light of the grey areas involved, I intend these patterns to serve as a useful analytic tool rather than precise descriptors of the surveillance law landscape. My classification of the various institutional decisions involved depends in part on judgments about what particular statutes accomplished—for example, responding to or attempting to preempt executive or judicial action. I do not attempt to correlate the statutes with claims about what the legislature intended, as opposed to what a reasonable observer might perceive the legislature to have achieved. In addition, I am concerned here only with constitutional questions about the *selection* of rules for conducting surveillance activities, not constitutional questions about the *application* of rules for conducting surveillance activities in a particular factual situation. For example, I am interested in categorizing challenges raising whether use of a particular surveillance tactic *should be subject to a standard* of probable cause before a neutral magistrate, not challenges raising whether *that standard has been satisfied* in particular cases. Finally, for ease of describing the relevant patterns, I focus on federal rather than state surveillance activities.

1. Executive Rule-Selection

I begin with disputes focusing on *executive* rule selection—that is, where the executive branch adopts a surveillance practice in the absence of any legislative action or outside the contours of existing statutes. In other words, Congress has not specifically spoken with respect to the particular practice at issue (or so the executive claims). Rather, it is left to the executive in the first instance to decide whether the practice is sufficiently privacy-invasive to require judicial authorization (and, if so, what kind of authorization to seek) or whether it can risk proceeding without judicial involvement. When the executive seeks judicial authorization under a too-weak standard, it runs the risk that the authorizing court will reject the request or that a target will successfully challenge the standard after the fact. When the executive does not seek such authorization, it runs the risk that a target will challenge the practice and claim that prior judicial authorization was necessary.

Instances of executive rule-selection that ultimately triggered judicial decisions on the constitutionality of executive conduct include the following: certain wiretapping and eavesdropping activities until the Court's decisions in *Katz* (and *Berger v. New York*⁴⁸ in the immediately preceding term);⁴⁹ warrantless national security surveillance of purely domestic targets in the era prior to the *Keith* decision; the use of pen registers and similar devices before the Supreme Court's decision in *Smith v. Maryland*;⁵⁰ the use of covert video surveillance tactics in the absence of specific legislative authorization;⁵¹ and the implementation of the NSA's terrorist surveillance program outside of FISA's requirements.⁵²

2. Legislative Rule-Selection

The remaining patterns involve legislative rule-selection rather than executive rule-selection, but differ in terms of the conditions under which the legislature selects a rule, and thus the posture in which a court must consider the constitutionality of the rule.

a. *Reactive statutes*

In some cases, a legislature authorizes (or imposes limits upon) surveillance practices in the wake of a prior judicial ruling on the constitutional contours of government power. The statute is "reactive:" The

48. 388 U.S. 41 (1967).

49. This example is complicated, because the Communications Act of 1934 provided that "[n]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication." Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1104 (codified at 47 U.S.C. § 605 (1958)). Federal officials for decades interpreted the provision not to bar wiretapping itself, but rather to bar the introduction of wiretap-derived evidence and its fruits into court. See Freiwald, *Online Surveillance*, *supra* note 9, at 28–31 (discussing the pre-Title III history of wiretapping among state and federal officials).

50. 442 U.S. 735 (1979).

51. See *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992) (en banc); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504 (2d Cir. 1986); *United States v. Torres*, 751 F.2d 875, 882–84 (7th Cir. 1984); see also *infra* notes 109–10 and accompanying text.

52. *ACLU v. Nat'l Sec. Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *rev'd on other grounds*, 493 F.3d 644 (6th Cir. 2007). Executive conduct of this type can of course raise statutory as well as constitutional questions. In other words, the question may be not only whether the Fourth Amendment requires the executive to follow certain procedures, but also whether a statute requires it to do so. Opponents of the NSA's terrorist surveillance program not only claimed that the program violated the Fourth Amendment, but also that FISA (and thus separation of powers principles) precluded it.

legislature responds to the prior constitutional decision by defining the circumstances in which the practice is permissible, and the executive follows the legislatively prescribed procedures.

Reactive statutes can take two quite different forms, depending upon whether the initial judicial decision approves or disapproves of the executive practice that preceded it. If the initial judicial decision finds existing procedures inadequate, the legislature must attempt to meet whatever constitutional bar the court sets. In a sense, the statute *codifies* the standards the court has articulated. If, however, the initial judicial decision finds existing procedures fully adequate (as, for example, by determining that the executive conduct in question is not a “search” for Fourth Amendment purposes), the legislature may seek to provide more procedural protections than a court has deemed the Fourth Amendment to require. We might regard the statute as *corrective*—as intended to reset the level of privacy protection to what the legislature perceives to be a more appropriate level.

The Wiretap Act and arguably FISA fit the former category. Congress adopted each statute in the wake of a Supreme Court decision that directly limited executive discretion to use certain surveillance tactics—in particular, to acquire communications in which a target could reasonably expect privacy. The judicial decisions left some room for legislative discretion, but made clear that the Fourth Amendment required robust constraints on executive conduct. In the case of the Wiretap Act, the protections Congress set essentially tracked those the Supreme Court outlined in *Berger v. New York*.⁵³ The statute at issue in *Berger* had allowed court authorization of eavesdropping activities, but the Court found the statutory procedures deficient in several respects. First, although the statute required a showing of reasonable grounds to believe that the surveillance would reveal evidence of criminal activity, the statute failed to satisfy the Fourth Amendment requirement that the crime to be investigated, the place to be searched, and the persons or things to be seized be particularly described.⁵⁴ Second, the statute imposed no limitations on which conversations could be seized or the duration of the surveillance, nor did it require termination of surveillance activities once the goals of the surveillance were met.⁵⁵ Third, the statute allowed law enforcement officials to secure renewal of a surveillance order on the basis of the initial showing.⁵⁶ Fourth, the statute did not provide for prior notice of the search

53. 388 U.S. 41 (1967).

54. *Id.* at 55–56.

55. *Id.* at 59–60.

56. *Id.* at 59.

to the subject of the surveillance and required no showing of exigency to justify the lack of notice.⁵⁷ Finally, the statute did not provide for a “return” on the warrant to a judge, “thereby leaving full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties.”⁵⁸

With the Wiretap Act, Congress sought to overcome each of these deficiencies. The Wiretap Act requires that the application specify the offense being investigated, the nature and location of the facilities where the communications are to be intercepted, and a particular description of the communications sought to be intercepted.⁵⁹ To grant the order, the court must find probable cause to believe that a particular enumerated offense is being committed and that targeting the specified facility will yield particular communications concerning that offense.⁶⁰ Congress dealt with *Berger*’s objection to the indeterminate length of surveillance under the New York statute by providing that orders may authorize surveillance only as long as necessary for achievement of the objective, up to thirty days.⁶¹ A court may grant an extension, but only subject to the same showings and findings as the original order. The statute also requires a court to order officials to “minimize” the interception of communications unrelated to criminal activity.⁶²

In light of *Berger*’s objection that the New York statute required no showing of exigency to justify the lack of notice, the Wiretap Act requires a finding that normal investigative procedures are unlikely to be successful or are too dangerous, and generally requires notice to the target of the investigation within ninety days of the termination of the surveillance.⁶³ Finally, Congress required law enforcement officials to take a variety of steps that provide the functional equivalent of a return to a judge. For example, the Wiretap Act requires law enforcement officials to record intercepted communications and to make the recordings available to the judge.⁶⁴ The statute also authorizes a judge to require periodic reports on the progress of the surveillance.⁶⁵

The circumstances surrounding FISA’s passage were slightly different, because the Supreme Court never spoke directly to the question whether warrantless national security surveillance of a *foreign* power or its agent

57. *Id.* at 60.

58. *Id.*

59. 18 U.S.C. § 2518(1)(b) (2006).

60. *Id.* § 2518(3).

61. *Id.* § 2518(5).

62. *Id.*

63. *Id.* §§ 2518(3)(c), (8)(d).

64. *Id.* § 2518(8)(a).

65. *Id.* § 2518(6).

violated the Fourth Amendment.⁶⁶ In *Keith*, however, the Court clarified that national security surveillance of a *domestic* target must comply with the Fourth Amendment. The Court acknowledged both that Congress could tailor specific statutory requirements to the peculiarities of national security surveillance⁶⁷ and that Congress could properly place the power to review surveillance applications in a specially designated court.⁶⁸ Although Congress never took up the Supreme Court's invitation to legislate distinct standards for national security surveillance of a domestic target, it enacted in FISA a special framework for surveillance of a foreign power or an agent of a foreign power.⁶⁹ More specifically, it established a specialized court, the FISC, to hear applications for electronic surveillance within the United States to gather foreign intelligence information.⁷⁰ In light of the *Keith* court's acknowledgement that special standards could be appropriate even for national security surveillance of domestic targets, FISA can be understood as Congress's attempt to map the Court's reasoning in *Keith* onto foreign intelligence gathering.⁷¹

66. In post-*Keith* cases involving warrantless surveillance against foreign powers or their agents to gather foreign intelligence information, three courts of appeals upheld the government's activities. See *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425 (5th Cir. 1973). A plurality of the Court of Appeals for the D.C. Circuit, however, addressing an issue not squarely presented in the case before it, questioned whether there could be any "foreign intelligence" exception to the warrant requirement. See *Zweibon v. Mitchell*, 516 F.2d 594, 613 (D.C. Cir. 1975) (en banc) (plurality opinion).

67. *Keith*, 407 U.S. 297, 322–23 (1972) (recognizing that standards differing from those governing electronic surveillance in criminal cases "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens").

68. *Id.* at 323.

69. See 50 U.S.C. §§ 1801–12 (2006 & Supp. III 2009).

70. See *id.* §§ 1803(a), (a)(6)(A)–(B). The term "electronic surveillance" has a complex definition, but essentially regulates acquisition of the contents of communications through the monitoring of persons or the installation of surveillance devices within the United States. *Id.* § 1801(f); see Bellia, *supra* note 47, at 430 n.33. Rather than requiring a showing of probable cause that a crime has been, is being, or will be committed, or that targeting the specified facilities will yield communications relating to a crime, FISA requires a showing of probable cause that the surveillance target is a "foreign power" or an "agent of a foreign power," and that the facilities are about to be used by such a power or agent. 50 U.S.C. § 1804(a)(4). There is substantial but not complete overlap between activities that make a target a foreign power or agent of a foreign power and those that constitute criminal activity. See Bellia, *supra* note 47, at 441.

71. Portions of the USA Patriot Act Improvement and Reauthorization Act, Pub. L. No. 109-177, 120 Stat. 192 (2006), provide another example of a congressional effort to respond to constitutionally-based judicial regulation of communications surveillance tactics. In September 2004, a district court held unconstitutional section 2709 of the Stored Communications Act, which authorized FBI investigators to issue "national security letters" compelling

Several statutes fall within the second, “corrective” category of reactive statutes—that is, providing additional statutory protection in response to a judicial decision that approves executive conduct undertaken with few procedural protections. As noted earlier, ECPA’s pen/trap provisions were in part a legislative response to the Supreme Court’s decision in *Smith v. Maryland*.⁷² The Court’s holding would have permitted federal and state officials (absent statutory constraints) to use pen registers and similar devices without prior judicial authorization. The pen/trap device statute is one of several statutes in which Congress sought to restore a measure of procedural protection to activities that the Supreme Court deemed not to constitute a search for Fourth Amendment purposes.⁷³

b. Proactive statutes

In some cases, Congress has not awaited a judicial decision regarding whether a particular executive tactic is constitutional; instead, it has sought to preempt the executive’s use of a particular tactic (and, by extension, a court’s assessment of it) by selecting the rule itself. Within this broad category of “proactive” statutes, it is helpful to distinguish further between two types: “modernizing” statutes—statutes that update surveillance law in

communications service providers to disclose certain transactional records concerning their subscribers. *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated on other grounds sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006). Although the court did not question the FBI’s authority to issue such letters, the statute contained a problematic nondisclosure provision prohibiting the recipient of an NSL from disclosing the existence of an NSL to any person. The district court concluded that the nondisclosure provision barred an NSL recipient from consulting an attorney to comply with the terms of the NSL, that the provision therefore violated the First and Fourth Amendments, and that the provision was not severable from the remainder of the statute authorizing the issuance of NSLs.

The NSL provision was among the several provisions amended when Congress took up reauthorization of the USA Patriot Act following the December 31, 2005, sunset date. More specifically, the USA Patriot Act Improvement and Reauthorization Act loosened the nondisclosure provision (as well as similar provisions in statutes authorizing NSLs in different contexts) to allow disclosure to an attorney and other persons necessary for compliance with the NSL. USA Patriot Improvement and Reauthorization Act § 116, 120 Stat. at 213 (codified at 18 U.S.C. § 2709(c) (2006)). The act also provided statutory authorization for an NSL recipient to challenge the scope of the NSL in court. *Id.* § 115, 120 Stat. 211 (codified at 18 U.S.C. § 3511).

72. 442 U.S. 735 (1979).

73. Other examples, less directly relevant to a discussion of communications surveillance tactics, include the Right to Financial Privacy Act, 12 U.S.C. §§ 3401–22 (2006) (responding to the Court’s decision in *United States v. Miller*, 425 U.S. 435 (1976), finding no expectation of privacy in bank records), and the Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (2006) (responding to the Court’s decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978)). See Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753–60 (2005); Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 916–17 (2004).

light of technological developments—and “crisis response” statutes—statutes that respond to a perceived investigative or intelligence failure by authorizing particular surveillance techniques thought lacking in existing law.

Modernizing statutes. Legislation updating surveillance law in light of technological developments might include both provisions designed to *limit* the use of particular surveillance techniques, on the theory that the law has not caught up with technological developments; and provisions designed to *overcome technological obstacles* to surveillance or to extend existing surveillance regimes to new technologies.

ECPA was designed to bring surveillance law authorities into line with technological developments.⁷⁴ The first portion of that statute amended the Wiretap Act, which initially protected only wire and oral communications, to cover interception of electronic communications as well.⁷⁵ The second segment of the statute, the SCA, established independent protections for stored wire and electronic communications.⁷⁶

These portions of ECPA reflect Congress’s recognition that development and adoption of new communications technologies depended upon public perceptions that such communications were secure from private and governmental interception.⁷⁷ The amendments to the Wiretap Act put electronic communications on nearly the same footing as wire and oral communications.⁷⁸ Similarly, the purpose of the SCA was to make stored

74. See, e.g., 131 Cong. Rec. 24,365–66 (1985) (statement of Sen. Leahy); *id.* at 24,396 (1985) (statement of Rep. Kastenmeier). For a fuller discussion of ECPA’s goals, see Brief on Rehearing En Banc for Senator Patrick J. Leahy as Amicus Curiae Supporting the United States and Urging Reversal, *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc) (No. 03-1383).

75. Electronic Communications Privacy Act of 1986, §§ 101–11, 100 Stat. 1848, 1848–59 (codified as amended at 18 U.S.C. §§ 2510–21 (2006 & Supp. III 2009)).

76. Electronic Communications Privacy Act §§ 201–02, 100 Stat. at 1860–68 (codified as amended at 18 U.S.C. §§ 2701–09, 2711–12 (2006 & Supp. III 2009)).

77. See, e.g., S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559; H.R. REP. NO. 99-647, at 19 (1986).

78. As a concession to the Justice Department, the amendments did not apply all features of the Wiretap Act to electronic communications, but they came close. See S. REP. NO. 99-541, at 23, *reprinted in* 1986 U.S.C.C.A.N. at 3577. There are three primary differences. First, § 2516(1) specifies the range of federal felonies for which government officials can seek orders to engage in surveillance of wire and oral communications. Although that list has grown considerably since the Wiretap Act’s enactment in 1968, it does not encompass all federal felonies. Under § 2516(3), however, law enforcement officials are authorized to seek Title III orders for surveillance of electronic communications in connection with any federal felony. Second, § 2516(1) also requires approval of certain high-level officials in the Justice Department before a request for surveillance of wire and oral communications can be sought from a court. No similar statutory restriction exists in § 2516(3) for surveillance of electronic communications, although the Justice Department has abided by such a restriction as a matter of

communications less vulnerable to unauthorized acquisition, while preserving law enforcement access to such communications.⁷⁹

ECPA also included examples of provisions designed to overcome technical impediments to surveillance. Section 106(d)(3), for example, added a provision loosening one of the particularity showings required for a Title III order, thus permitting “roving” surveillance where agents could demonstrate evidence that a target’s activities would otherwise thwart surveillance.⁸⁰ Eight years later, Congress dealt more directly with the perceived problem of technical developments eroding surveillance capabilities. CALEA, adopted in 1994, facilitated otherwise lawful surveillance orders by requiring telecommunications providers to design their systems to accommodate requests to intercept communications or obtain call identifying information associated with those communications.⁸¹

Portions of the USA Patriot Act perhaps provide a final example of a modernizing statute. Although Congress clearly sought to respond to some perceived gaps in surveillance law in the wake of the September 11, 2001, attacks, some portions of the statute had been discussed and proposed for years prior to those attacks. For example, the USA Patriot Act extended the pen/trap device statute to cover addressing and signaling information associated with electronic communications.⁸² Government agents had previously sought such information through requests that courts issue orders under the pen/trap device statute,⁸³ despite language ostensibly limiting that statute’s reach to wire communications.⁸⁴ Although no court had yet

policy. Finally, §§ 2515 and 2518(10) bar the use in evidence of wire and oral communications obtained in violation of the statute or in violation of a Title III order. No statutory suppression remedy exists for interception of electronic communications in violation of the statute.

79. The legislative reports accompanying ECPA acknowledged the legal uncertainty surrounding whether and how the Fourth Amendment might protect such communications. *See Bellia, supra* note 23, at 1413 (discussing conflicting views of whether subscribers retain an expectation of privacy in communications in the hands of a third party).

80. Electronic Communications Privacy Act § 106(d)(3), 100 Stat. at 1857 (codified as amended at 18 U.S.C. § 2518(11) (2006)).

81. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, 4280 (codified at 47 U.S.C. § 1002(a)(1)–(2) (2006)). For discussion of the statute’s enactment and implementation, see Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Breakup of AT&T*, 51 STAN. L. REV. 1049 (1999); Freiwald, *supra* note 31.

82. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288–89.

83. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t*, 97 NW. U. L. REV. 607, 633–34 (2003).

84. More specifically, the original statute defined a pen register as a device that “records or decodes electronic or other impulses which identify the *numbers dialed* or otherwise transmitted on the telephone line to which such device is attached.” 18 U.S.C. § 3127(3) (2006)

rejected the government's interpretation, the Justice Department included a codification of this interpretation in a package of measures proposed in response to the September 11 attacks.⁸⁵

Crisis response statutes. Proactive legislative responses to perceived investigative or intelligence failures would likely include several of the amendments to FISA. As first enacted in 1978, FISA covered only *electronic surveillance* of foreign powers or agents of foreign powers.⁸⁶ In a series of amendments in the 1990s, Congress added three new titles to FISA, one allowing the FISC to approve physical searches,⁸⁷ one allowing the FISC to approve the use of pen registers and trap-and-trace devices,⁸⁸ and one allowing the FISC to approve the compelled production of certain business records.⁸⁹ Each title responded to particular intelligence failures that the executive identified or that Congress perceived (or to concerns that government tactics undertaken without judicial authorization would subsequently be rejected in court).⁹⁰ For this Essay's focus on

(emphasis added). On the other hand, the statute defined a trap-and-trace device as a device to capture the "originating number" from which "a wire *or electronic* communication was transmitted." *Id.* § 3127(4) (emphasis added).

85. Consultation and Discussion Draft Bill to Combat Terrorism and Defend the Nation Against Terrorist Acts, and for Other Purposes (Sept. 19, 2001), *available at* http://epic.org/privacy/terrorism/ata2001_text.pdf.

86. Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783, 1793 (1978).

87. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1994) (codified as amended at 50 U.S.C. §§ 1821-29 (2006 & Supp. III 2009)).

88. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2405 (codified as amended at 50 U.S.C. §§ 1841-46 (2006 & Supp. III 2009)).

89. Intelligence Authorization Act for Fiscal Year 1999, § 602, 112 Stat. at 2410 (codified at 50 U.S.C. § 1862 (2000)). The amendment initially covered compelled production of travel-related business records, but was broadened in the USA Patriot Act to cover production of "tangible things" held by a third party. *See* USA Patriot Act § 215, 115 Stat. at 287 (codified as amended at 50 U.S.C. §§ 1861-62 (2006 & Supp. III 2009)) (deleting former §§ 1861-63 and adding new §§ 1861-62 authorizing orders to compel production of tangible things).

90. For example, the physical search provisions arose after government officials conducted covert physical searches without judicial authorization during their investigation of spying accusations against Aldrich Ames. The Justice Department apparently feared that a court would question the legality of such searches in a criminal trial against Ames. *See* S. REP. NO. 103-296, at 40 (1994). Ames's guilty plea obviated the need for a court to consider the issue, but the Justice Department sought an amendment to FISA to provide an avenue for such searches to occur pursuant to a FISC order. *Id.* The physical search provisions of FISA apparently can serve as a basis for certain forms of communications surveillance, in that government officials can use them to obtain copies of stored communications from service providers.

The provision authorizing agents to seek orders from the FISC compelling disclosure of certain business records may have arisen indirectly from the 1995 Oklahoma City bombing. At the time of the bombing, which some investigators initially theorized could be the work of foreign terrorists, there was no mechanism to compel production of business records (such as truck rental records) in an investigation involving an agent of a foreign power or an

communications surveillance tactics, the most relevant of these titles is the 1998 amendment authorizing the FISC to approve requests for the use of pen registers and trap-and-trace devices. The pen register and trap-and-trace amendment followed an incident in which investigators seeking the source of certain hacking activities that appeared to originate overseas could not get a foreign intelligence-related order to trace those activities without meeting the full requirements of FISA.⁹¹ The amendment thus created for foreign intelligence investigations an authorization procedure similar to that available through adoption of the criminal pen/trap statute in 1986.⁹² Under the new provision, investigators could request from the FISC an order permitting the use of a pen register or trap-and-trace device on a lower predicate than was required for the gathering of the contents of communications.⁹³

Portions of the USA Patriot Act also serve as obvious examples of the crisis response model. Among the Act's provisions were several responding to perceived intelligence failures in connection with the September 11 attacks. Perhaps the most controversial of these provisions was the provision dismantling the "wall" that separated criminal investigators and counterintelligence investigators within the Justice Department and the Federal Bureau of Investigation in investigations involving FISA.⁹⁴ The USA Patriot Act similarly loosened restrictions in the Wiretap Act on the sharing of information among agencies. Before September 11, the Justice Department had construed a Wiretap Act provision authorizing law enforcement officials to share intercepted communications with "another

international terrorist. See S. REP. NO. 105-185, at 28-29 (1998); cf. Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1329 (2004). The amendment thus allowed investigators to apply for an order requiring disclosure of travel-related records, such as rental car records, storage facility records, and so on. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410 (codified at 50 U.S.C. § 1862 (2000)); see *supra* note 89 (noting expansion of provision).

91. The incident, which occurred in February 1998, allegedly involved an Israeli teenager acting in concert with two American teenagers. See *Putting a Face on "Analyzer": The Alleged Teen Pentagon Hacker is Called Brilliant But Dangerous*, REUTERS (Mar. 20, 1998).

92. S. REP. NO. 105-185, at 27-28.

93. Other amendments to FISA likewise responded to specific investigative incidents, including a 2000 enactment (1) requiring the Attorney General, upon the request of certain high-level officials (including the Director of the FBI), personally to review a FISA application; and (2) specifying that the FISC could consider a target's past activities in determining whether there is probable cause to believe that the target is a foreign power or agent of a foreign power. See Intelligence Authorization for Fiscal Year 2001, Pub. L. No. 106-567, §§ 601-02, 114 Stat. 2831, 2850-52 (2000). These changes responded to a perceived failure in the handling of the Wen Ho Lee matter. See S. REP. NO. 106-352 (2000).

94. See Bellia, *supra* note 47, at 452-56; *infra* notes 131-39 and accompanying text.

investigative or law enforcement officer”⁹⁵ restrictively. The provision permitted disclosure “to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.”⁹⁶ The Department of Justice concluded that criminal investigators could share information acquired under the Wiretap Act in order to acquire from intelligence officials information relevant to the criminal investigation.⁹⁷ Officials could not, however, turn the fruits of electronic surveillance over to intelligence agencies on a wholesale basis.⁹⁸ The USA Patriot Act added language specifically allowing disclosure of the fruits of Title III surveillance to intelligence officials and others.⁹⁹

A final example of a crisis response provision is the post-Patriot Act “lone wolf” amendment. As enacted, FISA defined the term “agent of a foreign power” to include individuals acting on behalf of a terrorist group, not simply individual terrorists.¹⁰⁰ As a result, to secure a FISA order for surveillance of a suspected terrorist, agents had to demonstrate a link between the target and a specific terrorist group. Immediately prior to the September 11 attacks, this requirement proved an impediment to FBI agents who wished to secure a FISA physical search order to examine the contents of a laptop seized from Zacharias Moussaoui, whose suspicious behavior at a Minnesota flight school had prompted investigators to arrest him for an immigration violation shortly before the attacks.¹⁰¹ Adopted in 2004 as part of a broader intelligence bill, the lone wolf amendment expanded FISA’s

95. 18 U.S.C. § 2517(1) (2006).

96. *Id.*

97. Memorandum from Randolph D. Moss, Ass’t Att’y Gen., Office of Legal Counsel, U.S. Dep’t of Justice, to Office of Intelligence Policy & Review, U.S. Dep’t of Justice, Sharing Title III Electronic Surveillance Material with the Intelligence Community, 2000 WL 33716983 (Oct. 17, 2000)

98. *Id.*; see also Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1181 n.236 (2004).

99. USA Patriot Act § 203(b), 115 Stat. at 280 (codified at 18 U.S.C. § 2517 (2006)) (allowing disclosure to “any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official” to assist the receiving official in the performance of his official duties).

100. See 50 U.S.C. § 1801(a)(4), (b)(1)(A), (b)(2)(C) (2006).

101. See Bellia, *supra* note 47, at 425; see also NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 274 (2004). In the immediate aftermath of the attacks, Moussaoui was thought to be the “missing” twentieth hijacker—the fifth member of the team assembled to hijack United Airlines Flight 93 out of Newark, which ultimately crashed in rural Pennsylvania. See Philip Shenon, *The 20th Suspect*, N.Y. TIMES, Oct. 16, 2001, at B5. More recent evidence suggests that the fifth member of that flight team was in fact intended to be Mohamed al Kahtani, who was refused entry into the United States on August 4, 2001. See 9/11 COMMISSION REPORT, *supra*, at 456 n.73 (identifying the Moussaoui as a potential substitute pilot for United Airlines Flight 93).

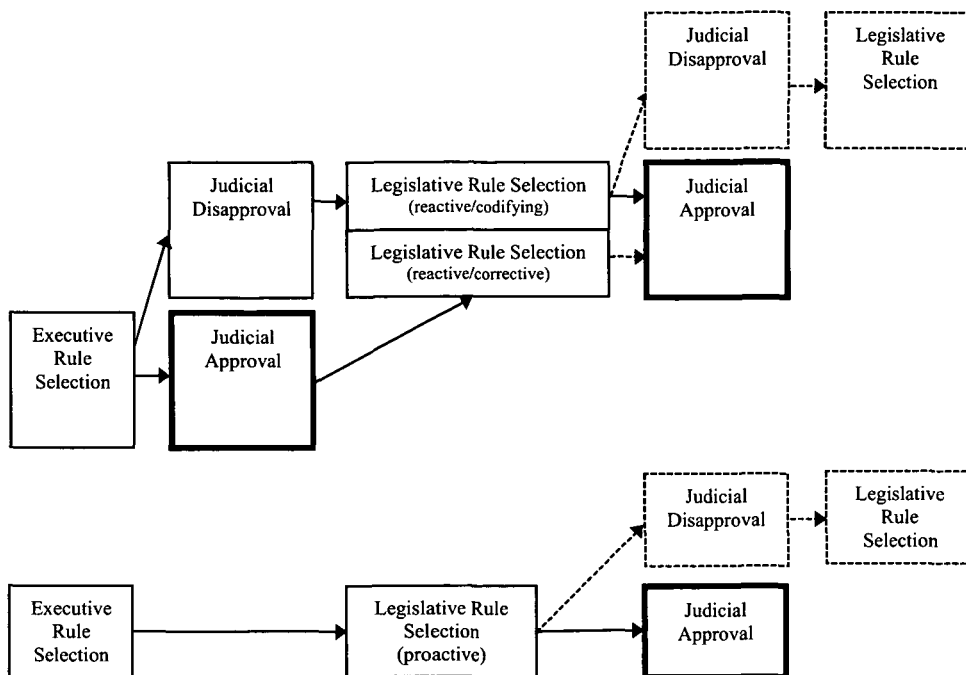
definition of the term “agent of a foreign power” to include an individual terrorist who is not shown to be working on behalf of a group.¹⁰² The lone wolf amendment thus relieved investigators of the burden of proving that one who engages in terrorist activities does so on behalf of a terrorist organization. Discussion of the amendment during hearings focused on the evidentiary burden that investigators faced in proving a connection with a terrorist organization in an era of looser, less centrally controlled terrorist groups.¹⁰³

C. *Understanding the Judicial Landscape*

Analyzing judicial outcomes through the lens of the institutional patterns outlined above permits a more nuanced view of executive, legislative, and judicial roles in regulating surveillance tactics. The graphics below reflect different postures in which a court might be called upon to assess a government investigator’s use of a particular surveillance technique. Each graphic presumes that the executive branch chooses in the first instance what procedures, if any, to follow before engaging in communications surveillance. If a court reviews the executive’s implementation of whatever rule it selects, the legislature might react to the judicial decision, and a further challenge to the executive’s implementation of the *legislatively* selected rule will follow. In other cases, the legislature will respond proactively to the executive’s rule selection before a court has acted, and judicial review will only follow once the executive implements the legislatively chosen rule.

102. More specifically, the measure broadened the definition of “agent of a foreign power” to include any non-U.S. person who “engages in international terrorism or activities in preparation therefore [sic].” Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C. § 1801(b)(1)(C) (2006 & Supp. III 2009)).

103. See, e.g., *Amendments to the Foreign Intelligence Surveillance Act: Hearings on S. 2586 and S. 2659 Before the S. Select Comm. on Intelligence*, 107th Cong. 14–19, 20–21 (2003) (statement and testimony of Marion E. “Spike” Bowman, Deputy General Counsel, FBI).



To the extent that normative arguments about how courts and Congress *should* regulate surveillance rest on an assessment of how courts have treated constitutional challenges to communications surveillance tactics since *Katz*, the patterns prove helpful in evaluating those assessments. The premise among judicial abdication scholars is that the surveillance law landscapes reflects judicial under-enforcement of Fourth Amendment guarantees; the premise among legislative supremacy scholars is that the surveillance law landscape reflects appropriate judicial deference. Yet to evaluate claims about under-enforcement or deference, it becomes necessary to know more about what precisely a court is evaluating. Judicial evaluation of the constitutionality of a surveillance tactic can arise in response to implementation of a rule selected by the executive, a rule selected by the legislature to meet or exceed the contours of a judicial decision (a codifying or corrective statute), or a rule selected by the legislature in an effort to be proactive (to modernize surveillance authorities or respond to a crisis). It is not surprising to find different levels of judicial intervention depending on the phase in which the claim arises.

A set of claims that Professor Kerr, who argues for legislative supremacy in surveillance law, makes about deference illustrates scholars' tendency to generalize about judicial responses in quite different circumstances. As

evidence of a trend of judicial deference, Professor Kerr notes¹⁰⁴ that: (1) Congressional action followed soon after the *Berger*, *Katz*, and *Keith* decisions, and statutory regulation thus supplanted judicial regulation of the techniques involved; (2) post-*Berger* and *Katz* challenges to the Wiretap Act have failed, including both facial challenges¹⁰⁵ and challenges to specific statutory gaps (such as the exclusion of cordless phones from the statute until 1994¹⁰⁶); and (3) courts have regulated covert video surveillance tactics not by articulating new standards but by relying upon those already appearing in the Wiretap Act, despite the fact that the statute clearly exempts video surveillance.¹⁰⁷ As a descriptive matter, we could characterize these developments differently—with different implications for a normative assessment of the respective roles of legislatures and courts in regulating surveillance activities.

1. Executive Rule-Selection

First, when a court evaluates the executive's choice of a rule to govern a particular surveillance tactic before the legislature has spoken—when it evaluates executive action—it faces a different question of deference than it does in response to implementation of a legislatively chosen rule. Neither a court nor a legislature has assessed the privacy implications of the practice. Unsurprisingly, we do find some significant judicial activity in this category. *Berger*, *Katz*, and *Keith* provide examples of such activity, as does the district court decision declaring the NSA terrorist surveillance program unconstitutional.¹⁰⁸ Legislative action, of course, followed the *Berger*, *Katz*,

104. I leave aside here two arguments that I believe have little bearing on analysis of the relative roles of courts and legislatures in communications surveillance law: that courts refused to imply a civil remedy for a violation of the Wiretap Act in *Adams v. City of Battle Creek*, and that even outside of the core concern of domestic wiretapping, courts have looked to statutory law in permitting compliance with foreign statutes to satisfy Fourth Amendment reasonableness standards. See Kerr, *supra* note 10, at 853. The first example does not involve a threshold determination that a reasonable expectation does or does not apply and is thus inapposite. Even if the foreign law examples involve deference to statutory law, they do not advance Professor Kerr's central claim that courts have historically deferred to *congressional* judgments about surveillance law.

105. See Kerr, *supra* note 10, at 850 (“The judiciary’s deferential stance began with the case law that followed the passage of Title III.”).

106. *Id.* at 852 (“[T]he courts refused to say that the Fourth Amendment covered the ground that Congress had not protected: instead, the courts deferred to Congress’s judgment and held that such calls were not covered by the Fourth Amendment.”).

107. See 18 U.S.C. § 2510(1), (2), (12) (2006) (defining “wire,” “oral,” and “electronic” communications).

108. *ACLU v. Nat’l Sec. Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *rev’d on other grounds*, 493 F.3d 644 (6th Cir. 2007).

and *Keith* decisions, and case-by-case adjudication of surveillance techniques yielded to the Wiretap Act and FISA. But judicial decisions framed that legislation, and the reactive nature of the legislation makes it difficult to characterize courts' posture in this context as deferential.

Similarly, the covert video surveillance cases reflect courts' determination that the technique invades a reasonable expectation of privacy and that agents must meet stringent procedural requirements to use it.¹⁰⁹ Congress placed video surveillance outside of the ambit of the Wiretap Act, but courts imposed the Wiretap Act's requirements anyway. To be sure, courts adopted the Wiretap Act's requirements rather than developing new judicial standards.¹¹⁰ Adoption of those requirements, however, was premised upon the threshold determination that the technique invades a reasonable expectation of privacy. That determination is one that Professor Kerr implicitly expects, if not explicitly urges, courts to leave to the legislature. As a descriptive matter, then, the example is not one of deference to legislative choices.

Of course, courts do not always respond to executive rule-selection by demanding stringent procedures. For example, many scholars have criticized the Supreme Court's determination in *Smith v. Maryland* that the Fourth Amendment permits warrantless use of pen registers and similar devices.¹¹¹ Because my primary goal here is to set the stage for a discussion of institutional competence in surveillance questions, I am less interested in the merits of this dispute than in what it tells us about the relative roles of courts and legislatures.¹¹² The *Smith* example in fact illustrates the tremendous power of a court's initial determination whether a surveillance tactic invades a reasonable expectation of privacy. Although Congress soon adopted standards that exceeded those that the Supreme Court found the Fourth Amendment to require, those standards did not remotely approximate the standards that would have prevailed had *Smith* been decided otherwise. In other words, the Court's decision in *Smith* obviated the need for Congress to provide more robust procedures. That Congress chose to exceed those the court required did not make it the primary architect of the surveillance law scheme; rather, the Court's Fourth Amendment determination established the framework within which Congress legislated.

109. See *supra* note 51 (citing cases).

110. Kerr, *supra* note 10, at 854.

111. See, e.g., Freiwald, *supra* note 31, at 949, 982–89; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1137–38 (2002).

112. I have discussed the shaky doctrinal underpinnings of *Smith v. Maryland* elsewhere. See Bellia, *supra* note 23, at 1397–1413.

2. Legislative Rule-Selection

a. Reactive statutes

Moving to *reactive* statutes, it is true as a descriptive matter that courts have often rejected constitutionally-based challenges to such statutes. The absence of successful constitutional challenges in this context, however, does not necessarily signal either judicial under-enforcement or judicial deference to legislative choices.

In the case of a codifying statute, when a court has disapproved of a particular executive tactic and the legislature responds by implementing the judicial decision, further judicial intervention on constitutional grounds seems quite unlikely, especially if there is evidence that the legislative branch (and the executive branch) fully considered the constitutional issues in light of the court's pronouncements. The Wiretap Act, as noted, was drafted with *Berger* very much in mind, and the statute's formidable statutory protections match or exceed features of a warrant.¹¹³ The failure of challenges to the statutory scheme may reflect some deference to Congress's assessment of constitutional requirements, despite courts' claims not to give decisive weight to such interpretations. Or that reluctance may simply reflect the fact that Congress (and its partners in the executive branch) interpreted and applied the same body of constitutional law as the courts and correctly assessed the constitutional issue.

Similarly, if a court approves of particular executive conduct undertaken with few procedural safeguards, it is unlikely to invalidate a reactive legislative rule that seeks to correct the judicial decision by enhancing those safeguards.

In short, very little can be gleaned from the absence of successful constitutional challenges to reactive statutes. Whether such examples reflect judicial under-enforcement links back to the judicial decision on the rule selected by the executive in the first instance. Deference to legislative decisions may be a factor in such cases, but it is difficult to isolate legislative deference in such cases because the legislative choices are intertwined with the judicial decisions that preceded them.

b. Proactive Statutes

Proactive statutes raise more difficult questions. Here, Congress seeks to develop a Fourth Amendment-compliant framework without a prior judicial

113. See *supra* notes 53–65 and accompanying text; Kerr, *supra* note 10, at 851; see also Bellia, *supra* note 23, at 1388–91 (describing protections).

determination whether use of a surveillance tactic invades a reasonable expectation of privacy. If Fourth Amendment challenges are unsuccessful in this context, it cannot be because courts and the political branches are simply relying on the same clearly authoritative sources of law to assess the issue. No well-developed law exists. As a result, it becomes difficult to distinguish instances of appropriate judicial deference to Congress from inappropriate judicial under-enforcement of Fourth Amendment guarantees.

Within the two categories of “proactive” statutes, however, it is possible to identify certain points at which judicial under-enforcement is a risk. Consider the two types of judgments that Congress must make in drafting a modernizing statute. Congress first must make factual judgments about the state of technology; it then must make normative judgments about how much privacy protection is warranted in light of those facts. When a court initially considers the constitutionality of a modernizing statute, it is unlikely to question Congress’s recent factual judgments. Rather, its main task will be to evaluate Congress’s judgment about how much privacy protection is warranted—that is, about whether users of a particular communications technology can reasonably expect privacy in that technology.

There are a number of reasons why courts might be unlikely to dislodge that judgment. First, if a court applying the reasonable expectation of privacy test takes a positive approach rather than a normative one—asking what privacy users *do* expect rather than what they are *entitled* to expect—then a court’s inquiry necessarily becomes an empirical one, requiring consideration of (among other things) society’s perceptions of the vulnerability of communications to unauthorized acquisition. Engaging in such an inquiry with respect to an emerging communications medium requires an empirical analysis by a court to assess what society’s perceptions are.¹¹⁴ Even if a court were equipped to undertake this empirical assessment, inquiring into the vulnerability of a communications medium slants the inquiry against constitutionally-based judicial regulation of new technology, for it will be rare for society not to perceive a new communications medium to be vulnerable.

As time goes on, moreover, it may become increasingly difficult for a court to dislodge erroneous congressional judgments about the path of technology. Assume that the path of technology veers away from Congress’s initial predictions—and thus calls into question congressional decisions about how much privacy protection is warranted. Assume also

114. Freiwald, *First Principles of Communications Privacy*, *supra* note 9, ¶¶ 22–45 (discussing difficulties of the positive versus normative inquiry into the reasonableness of an expectation of privacy).

that courts rejected initial constitutional challenges to the statutory scheme. Whether early decisions about the constitutionality of a statute explicitly or implicitly deferred to Congress's judgment on the underlying facts about the state of technology, or merely came to the same conclusion as Congress did, those decisions will be difficult to dislodge once the statute has been on the books and has gone unquestioned for many years. To hold that the statutory scheme sets inadequate procedures, the court must question a factual judgment that was unquestionable at the time it was made, or generate new empirical assessments about society's perceptions of the medium's vulnerability.

In short, when properly presented with a challenge to a modernizing statute, a court may simply be deferring to Congress's superior expertise to set flexible and adequately protective rules. On the other hand, the case may be one of judicial under-enforcement. Over time, moreover, the facts may shift such that appropriate deference becomes under-enforcement, as the nature of the reasonable expectation of privacy inquiry and the fact that a statute has been on the books for many years combine to make the statute difficult to dislodge.

The SCA's framework for compelled disclosure of the contents of communications illustrates some of these difficulties. As noted earlier, the SCA permits government officials to compel a service provider to disclose a subscriber's communications under certain circumstances. For communications in "electronic storage" for 180 days or less, a warrant requirement applies.¹¹⁵ For communications not in "electronic storage," a court order issued on standards short of those required for a warrant will suffice.¹¹⁶ The government's traditional view was that the "electronic storage" category encompassed a relatively small category of electronic communications—not all e-mails, but only those communications not yet downloaded from the provider's server.¹¹⁷ All other messages, including messages opened by the subscriber but retained on the server and sent messages retained on the server, could be retrieved without a warrant.¹¹⁸

115. 18 U.S.C. § 2703(a) (2006 & Supp. III 2009).

116. *Id.* § 2703(b), (d).

117. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 123 (3rd ed. 2009) [hereinafter CCIPS MANUAL], *available at* <http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf> (stating that "[electronic storage] does not include post-transmission storage of communications").

118. *Id.* at 124 ("Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in 'temporary, intermediate storage' and is not stored

Such messages, in the government's view, were communications held or maintained by a remote computing service—a category less well protected by the statute.¹¹⁹

At the time of ECPA's adoption, the narrow interpretation of the term "electronic storage" might have been unproblematic. In 1986, electronic communications were not widely used for personal purposes.¹²⁰ At the time, moreover, the term "remote computing service" fit comfortably with the ways in which businesses might treat certain records. Because computing capacity and storage was still relatively expensive, a business might outsource certain processing and data storage tasks, and the statute treated a company that performs such storage and processing services as the provider of a "remote computing service."¹²¹ Communications held by a remote computing service would typically be business records for purposes of the Fourth Amendment—that is, records held by a third party and not communications in which a subscriber could have a reasonable expectation of privacy.¹²²

In short, the SCA contemplated both short-term storage of communications with an electronic communications service, and longer-term storage of records with a remote computing service. The technological environment within which the SCA's distinctions apply has changed dramatically, inasmuch as *long-term* storage of *personal* communications is now a norm.¹²³ In 1986, it was likely that users would have had to take affirmative steps to retain e-mail messages they already accessed.¹²⁴ Storage is now extremely cheap, and e-mail services such as Gmail base their entire business models on the proposition that users can and should have access to a searchable database of *all* of their e-mails—read or unread. If the Justice Department's interpretation still prevails, however, all opened or sent

incident to transmission. . . . By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in 'electronic storage.'" (citation omitted).

119. *Id.* at 126. The "remote computing service" category applies only if the provider offers services to the public. In other cases, a message in post-transmission storage would be unprotected by the SCA. *Id.*; see 18 U.S.C. § 2711(2) (2006) (defining "remote computing service" as an entity that provides computer storage or processing services "to the public").

120. See Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1567 (2004) (noting that e-mail users in 1986 were primarily academics, military personnel, and some business people).

121. 18 U.S.C. § 2711(2).

122. See *United States v. Miller*, 425 U.S. 435 (1976); see also Bellia, *supra* note 23, at 1397–1413 (discussing *Miller*); Mulligan, *supra* note 120, at 1569.

123. See Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 147–49 (2008).

124. Mulligan, *supra* note 120, at 1569.

messages that remain on systems like Gmail are not subject to the higher warrant-like protections of section 2703(a) of the SCA.

A court addressing a constitutional challenge to the Justice Department's interpretation faces a dilemma. The technical assumptions undergirding the original statute—that long-term storage of electronic communications would not occur, and that communications held by a remote computing service are easily classified as business records—no longer hold. Any court asked to approve a 2703(d) order for e-mail that, under the government's interpretation, is outside of the electronic surveillance definition implicitly passes on the constitutionality of the government's position. Yet that position, even if erroneous, will be difficult to dislodge. In the first case to squarely address the constitutionality of the government's position, *Warshak v. United States*, the government quite naturally pointed out that, in twenty years, no court had ever declared these provisions of the SCA unconstitutional.¹²⁵ The case law in this area remains unstable.¹²⁶ Indeed, it is interesting that the major limit on the government's conduct—at least before *Warshak*—came not from case-by-case adjudication in disputes involving criminal defendants, but (arguably erroneous) statutory construction in a *civil* dispute.¹²⁷

As with the other categories of statutes, I am less interested in the merits of the SCA dispute than I am in what it shows about the interplay of the legislative and judicial branches. A legislative supremacy scholar would argue that the absence until very recently of judicial intervention, and the current instability in the case law, demonstrates Congress's superiority in setting flexible and adequately protective rules for developing technologies. A judicial abdication scholar would detect under-enforcement. When the SCA is viewed as a modernizing statute, a third possibility suggests itself—that the shifting technological landscape has destabilized the structure of a statute that was once plausibly viewed as constitutional.

125. Brief for Defendant-Appellant United States at 14, *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007) (No. 06-4092) ("For twenty years, the Stored Communications Act has set forth the procedures for the government to follow to compel disclosure of e-mail, and no court has previously found it to be unconstitutional.").

126. Compare *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), and *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated on reh'g en banc*, 532 F.3d 521 (6th Cir. 2008), with *Rehberg v. Paulk*, 598 F.3d 1268, 1282 (11th Cir. 2010), and *In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail*, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009).

127. See *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003), *reh'g denied and opinion superseded*, 359 F.3d 1066 (9th Cir. 2004). For a discussion of the difficulties the *Theofel* court's opinion raises, see Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1335–38 (2005).

Crisis response statutes. In the other category of proactive statutes—those involving Congress’s response to a perceived gap in investigators’ surveillance authorities—we likewise see little constitutionally-based regulation. Again, however, we can identify specific challenges such statutes present for courts.

Like modernizing statutes, crisis response statutes reflect two distinct congressional judgments. The first is a judgment about whether a particular tactic is sufficiently invasive to require prior judicial authorization (and if so, on what standard). The second is a judgment about the urgency of the need for the investigative tool.

These judgments are so closely tied together—particularly on the foreign intelligence side—that a court inquiring into the first may end up unraveling the second. On the foreign intelligence side, the prevailing doctrinal test gives great weight to investigative needs. *Keith* explicitly contemplates that national security investigations may present “different policy and practical considerations from the surveillance of ‘ordinary crime’”¹²⁸ and contemplates that those considerations permit standards different from those governing surveillance in criminal cases, so long as those standards “are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.”¹²⁹ This test remains underdeveloped in the law and, as a result, operates as a fairly soft limit on congressional action.¹³⁰

Courts’ reluctance to question the constitutionality of the Patriot Act amendments to FISA illustrates the challenges of reviewing a crisis response statute in the foreign intelligence area. The Patriot Act amended FISA to permit surveillance to proceed on a national security official’s certification that a “significant purpose” of the surveillance, rather than “the purpose” of the surveillance, is to acquire foreign intelligence information. A pre-FISA decision, *United States v. Humphrey*,¹³¹ had held that warrantless surveillance was unlawful once the gathering of foreign intelligence was no longer the “primary purpose” of the surveillance, and had identified the point at which the “primary purpose” had shifted to criminal prosecution by conducting an evidentiary hearing to assess the involvement of criminal prosecutors in the case.¹³² Although FISA as enacted simply required certification as to “the” purpose of the surveillance, defendants challenging FISA surveillance drew upon the *Humphrey* case to

128. *Keith*, 407 U.S. 297, 322 (1972).

129. *Id.* at 322–23.

130. Bellia, *supra* note 47, at 449–52.

131. 456 F. Supp. 51 (E.D. Va. 1978).

132. *Id.* at 58–59.

argue that such surveillance could only proceed where the *primary* purpose of the surveillance was to obtain foreign intelligence information. Several courts of appeals invoked the primary purpose test in dicta in upholding FISA surveillance.¹³³

In 1995, the Attorney General adopted guidelines concerning the sharing of FISA-derived information between counterintelligence and criminal investigators and prosecutors within the FBI and the Justice Department.¹³⁴ These guidelines, which came to be known as the “wall” between counterintelligence and criminal investigators, were prompted in part by concern that a court following the *Humphrey* court’s logic would use contacts between such investigators to assess the purpose of FISA surveillance. That is, the guidelines were designed to minimize the use of FISA-derived information by criminal investigators, lest courts treat the involvement of criminal prosecutors as evidence that the primary purpose of the surveillance was to conduct a criminal investigation. After the Patriot Act altered FISA to permit certification of “a *significant* purpose” rather than “*the* purpose” to obtain foreign intelligence information, the FISC itself appended a modified version of the 1995 guidelines to orders approving surveillance requests. In other words, the FISC sought to reintroduce the “wall” that the Justice Department believed it could eliminate after passage of the USA Patriot Act.

When the Justice Department sought modification of the guidelines the FISC imposed, the FISC rejected its request. The FISC did not decide the case on constitutional grounds, and indeed claimed that the case raised no constitutional issue¹³⁵—even though the evolution of the 1995 guidelines could be traced back to a Fourth Amendment decision. The Foreign Intelligence Surveillance Court of Review (“FISCR”) reversed the FISC’s statutory holding, but also concluded that the proposed Justice Department guidelines did not violate the Fourth Amendment.¹³⁶ The FISCR observed

133. Bellia, *supra* note 47, at 454.

134. See Memorandum from Janet Reno, Attorney General, to Assistant Attorney General, Criminal Division; Director, FBI; Counsel for Intelligence Policy; and United States Attorneys, *Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations* (July 19, 1995), available at <http://www.fas.org/irp/agency/doj/fisa/1995procs.html>.

135. See *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 614 (FISA Ct. 2002) (en banc) (“The question before the Court involves straightforward application of the FISA . . . and raises no constitutional questions that need to be decided.”).

136. *In re Sealed Case*, 310 F.3d 717, 736, 746 (FISA Ct. Rev. 2002). More precisely, the court concluded that the new guidelines are constitutional when construed to permit use of FISA where the primary purpose of the surveillance or search is to obtain evidence of foreign intelligence crimes (as distinct from ordinary crimes). See *id.*

that the constitutional question “has no definitive jurisprudential answer.”¹³⁷ The reasonableness inquiry in any given case will turn on the differences between national security surveillance and surveillance related to ordinary crime.¹³⁸ Those differences include the government interest involved, the goals of the surveillance, the secrecy required, and the logistical challenges (such as the interrelationship of sources, precision with respect to the target, and the practical problems involved where activities are planned and conducted abroad).¹³⁹

If one considers the posture of the case before the FISC—one involving a court considering a Fourth Amendment challenge to a crisis response statute in the immediate aftermath of its enactment—the FISC’s holding is unsurprising. A crisis response statute reflects Congress’s assessment of urgent investigative demands, and that assessment will be difficult to second-guess in the immediate aftermath of a crisis. Again, the point here is not that the FISC’s decision is correct or incorrect. The point, rather, is that courts’ hands-off approach might reflect judicial deference to Congress’s superior ability to weigh privacy and law enforcement interests, or it might reflect under-protection of privacy interests in the face of urgent investigative demands.

3. Summary

Two key points emerge from this discussion. The first concerns the role of courts in regulating surveillance techniques. Observing that statutes predominate in communications surveillance law understates the role of courts. Judicial regulation in cases involving executive rule selection is both present and unsurprising. In addition, some judicial silence as to the constitutionality of surveillance can be explained by the reactive nature of the statutes involved, where courts have in fact largely driven the statute’s terms or Congress has sought to provide safeguards above those a court has found the Constitution to require. The second key point concerns how we might explain courts’ hands-off approach. The fact that courts have played a limited role in response to proactive statutes as well may reflect a welcome norm of judicial deference to legislative action. On the other hand, examining the surveillance law landscape in light of the patterns outlined above reveals certain risks of under-enforcement—in the case of modernizing statutes, a failure to dislodge assumptions about the path of

137. *Id.* at 746.

138. *See* Bellia, *supra* note 47, at 457.

139. *See id.* at 450–51 (culling these factors from *Keith* and subsequent decisions rejecting Fourth Amendment challenges to FISA).

technology, and in the case of crisis response statutes, a failure to isolate or properly weigh the importance of government interests.

II. FROM FIRST-ORDER TO SECOND-ORDER QUESTIONS IN SURVEILLANCE LAW

As Part I illustrated, calls for greater judicial and congressional involvement in regulation of communications surveillance law tend to understate the complexity of the judicial landscape in this area. Examining that landscape in light of the institutional patterns identified above reveals that the judicial abdication perspective and the legislative supremacy perspective understate the role of courts.

Although we can identify contexts in which courts have played a limited role, the normative significance of this fact is unclear. That is, we still face questions about how courts *should* behave and about the relative competence of legislatures and courts to set limits on executive surveillance tactics. The surveillance law patterns identified above can help guide this inquiry into institutional competence in at least two ways. First, examining the relative roles of courts and the legislature in regulating surveillance tactics reveals the particular risks of under-enforcement that *proactive* statutes present. Second, the patterns suggest the sequential and iterative nature of surveillance law, with decisions proceeding from executive rule selection, to a judicial or legislative decision, to another judicial or legislative decision, with the possibility of both constitutional and statutory questions. The institutional patterns thus reveal opportunities to explore how the decisions of one institution shape and constrain the decisions of the next. In short, discussions of institutional competence should not overlook the ways in which institutional *design* can shape the quality of decisions the various institutions will produce.

This Part fleshes out this claim. Section A begins by exploring institutional competence arguments through the lens of the institutional patterns identified in Part I. Section B seeks to disentangle the relationship between what we might call “second-order” design questions from the first-order preferences and constitutional constraints on which institutional competence arguments rely. Finally, Section C identifies and explores the categories of design choices likely to affect the quality of decision-making in this context.

A. *Comparative Institutional Competence*

As noted previously, scholars' views on what role courts *should* play in setting surveillance law rules implicitly or explicitly reflect arguments about institutional competence. Those scholars who would shift more decision-making to courts, for example, see Congress as having been captured by law enforcement interests on these issues.¹⁴⁰ Legislative supremacy scholars, in contrast, focus on how Congress can respond quickly to rapid technological changes, whereas courts' case-by-case decisions will necessarily involve a narrow and possibly outdated record.¹⁴¹

Institutional choice methodologies are, of course, controversial in many respects.¹⁴² Indeed, it is certainly possible to fault both judicial abdication scholars and legislative supremacy scholars for being insufficiently comparative in their analysis. Judicial abdication scholars focus on the pressures that law enforcement interests are likely to exert in Congress without asking whether courts have the tools to assess how technological changes will affect privacy and law enforcement interests.¹⁴³ Legislative supremacy scholars, in contrast, tend to focus on the legislature's speed and technical expertise without asking how the access and influence of law enforcement interests are likely to affect legislative outputs. It is beyond the scope of this Essay to fully engage that debate. Rather, taking it as a given that arguments about institutional competence are relevant to how we allocate decision-making authority in surveillance law, I seek to show that those arguments should account for how design choices affect the quality of judicial and legislative decisions.

A word about goal choice is in order at the outset. Because institutional competence arguments typically seek not to arrive at a legal rule, but rather to determine which institution is best positioned to do so, identifying the overarching policy goal that the legal rule is to serve is important. I identify this overarching goal as providing appropriate checks on executive discretion in the use of communications surveillance tactics; in theory, a comparative institutional analysis should identify which institution is best-positioned to set those checks. Although I believe that legislative supremacy and judicial abdication scholars would agree on this goal, the goal is often stated instead in terms of "balancing" privacy interests against legitimate law enforcement needs. Professor Susan Freiwald has pointed out that the

140. See, e.g., Swire, *supra* note 73, at 914 (likening law enforcement agencies to regulated industry); Swire, *supra* note 90, at 1348–50 (describing public choice realities of how surveillance legislation is enacted).

141. Kerr, *supra* note 10, at 864–82.

142. Cf. Solove, *supra* note 73, at 760.

143. See, e.g., Swire, *supra* note 73, at 914.

“balancing” metaphor is a pervasive but problematic one, in that it assumes that more information will in fact serve law enforcement needs and permits privacy invasions even when less restrictive means to accomplish law enforcement goals exist.¹⁴⁴ The policy goal as formulated above sidesteps the question whether privacy trade-offs actually serve law enforcement needs in favor of asking how the law can and should restrain executive choices in this area.

I now examine the competing institutional competence arguments in light of the institutional patterns identified in Part I.

1. Executive Rule-Selection

Institutional competence arguments about communications surveillance law tend to focus on the choice between *legislative* and *judicial* controls on executive action, without considering the possibility of the executive restraining its own conduct in some way. Focusing on cases involving executive-rule selection thus seem to add little to arguments about judicial competence, because those who believe that courts are in a better position than legislatures to police executive conduct certainly also believe that courts are better than the executive itself.

Executive rule-selection cases raise an interesting challenge for legislative supremacy scholars, however. If the thrust of the legislative supremacy position is that legislative regulation of surveillance tactics is preferable to judicial regulation, then courts should arguably decline to intervene in cases involving executive rule-selection, so as to leave the legislature with space to regulate. For example, in arguing that functional considerations should lead courts to be “cautious” in evaluating challenges to the use of new search technologies, Professor Kerr does not confine his claims to situations where Congress has already passed a (proactive or reactive) statute regulating the practice. That is, the call for “deference” or “caution” is in part a call to leave the legislature space to work.

In this context, however, the broad delegation to the executive of investigative powers means that judicial caution in favor of preserving legislative space essentially privileges the executive’s interpretation of its powers. Whether or not such an approach might be appropriate under a distinct assessment of institutional competence weighing the merits of executive self-regulation against judicial and legislative approaches, it is enough here to note that merely comparing legislative and judicial

144. Freiwald, *Online Surveillance*, *supra* note 9, at 19–20.

competencies (as legislative supremacy scholars do) is not enough to justify a rule of legislative supremacy.

2. Legislative Rule-Selection

Turning from situations involving executive rule-selection to situations involving legislative rule-selection allows two broad observations about institutional competence arguments. First, questions about institutional competence cut across statutory and constitutional issues. Once the legislature dictates surveillance law rules, courts may be called upon to evaluate the executive's implementation of those rules in light of the Fourth Amendment, but they will also be called upon to interpret the statute itself. An account that favors a statutory privacy framework to a Fourth Amendment framework bears the burden of establishing that, as a matter of institutional competence, (1) interposing a statute makes the court's constitutional task easier, and (2) courts are likely to be more successful at *statutory* construction in this area than they will be at *constitutional* construction. On the first point, it is true that interposing a statute may minimize the risk of judicial *over-enforcement* of the Fourth Amendment. As discussed in Part I, however, legislative and thus judicial under-enforcement is a significant risk in the case of proactive statutes. As to the second point, the difficulties that courts might have with technology-laden issues do not disappear when Congress adopts a statute governing use of the technique. And if Congress does not speak with clarity, the risks of judicial over-enforcement and under-enforcement *of the statute* still remain. Indeed, one could argue that the background operation of the Fourth Amendment can in fact improve statutory construction.

Consider, for example, the case of *United States v. Councilman*.¹⁴⁵ In that case, the United States sought to prosecute a service provider that had captured communications of its customers before transmitting them into users' mailboxes.¹⁴⁶ A key question was whether the provider's conduct amounted to an "interception" under the Wiretap Act. More specifically, the provider claimed that because it acquired the communications while they were briefly stored in its system before being transmitted to the user's mailbox,¹⁴⁷ the provider had not "intercepted" them within the meaning of

145. *United States v. Councilman*, 245 F. Supp. 2d 319 (D. Mass. 2003) (*Councilman I*), *aff'd*, 373 F.3d 197 (1st Cir. 2004) (*Councilman II*), *pet'n for reh'g en banc granted*, 385 F.3d 793 (1st Cir. 2004), *rev'd*, 418 F.3d 67 (1st Cir. 2005) (en banc) (*Councilman III*).

146. *Councilman I*, 245 F. Supp. 2d at 319.

147. *Councilman II*, 373 F.3d at 199–200.

the Wiretap Act. The district court agreed,¹⁴⁸ and the Court of Appeals for the First Circuit affirmed on the same reasoning.¹⁴⁹

As noted earlier, a number of courts have held that a non-contemporaneous acquisition of communications from storage is not an interception.¹⁵⁰ The *Councilman* courts, however, took the analysis one step further and held that even a *contemporaneous* acquisition of communications from a storage point *along the transmission path* is not an interception. If this interpretation were correct, then government officials could rely on the less stringent procedures of the SCA to compel production of a communication at any one of a number of points along its transmission path, rather than obtaining a Title III order.¹⁵¹ This interpretation undoubtedly has constitutional implications as well as statutory ones. Had the courts considered the constitutional implications of their approach, it seems unlikely that they would have reached the same result. The constitutional avoidance issue was briefed before the en banc First Circuit,¹⁵² which ultimately reversed the district court.¹⁵³

In short, to sustain functional arguments that the legislature is in a better position to regulate executive surveillance tactics, one must conclude that courts are better equipped for statutory construction than constitutional interpretation or, at a minimum, that the dangers of erroneous statutory construction are less significant than the dangers of erroneous constitutional interpretation. The interdependence of the constitutional and statutory frameworks, however, makes both arguments questionable.

The second observation that arises from legislative rule-selection cases is that legislative design choices can themselves limit courts' ability to resolve statutory or constitutional questions. Consider first the absence of a statutory suppression remedy for electronic communications under the Wiretap Act and for all communications under the SCA. The lack of a suppression remedy limits courts' ability to address questions of statutory interpretation—perhaps perpetuating impressions of judicial inability to

148. *Councilman I*, 245 F. Supp. 2d at 321.

149. *Councilman II*, 373 F.3d at 204.

150. See *supra* note 25 and accompanying text.

151. See, e.g., Brief on Rehearing En Banc for Senator Patrick J. Leahy as Amicus Curiae Supporting the United States and Urging Reversal at 10–11, *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc) (No. 03-1383), available at <http://www.cdt.org/wiretap/20041112leahy.pdf>; Supplemental Brief for Center for Democracy and Technology et al. as Amici Curiae in Support of the United States in Favor of Reversal at 1–4, *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc) (No. 03-1383), available at <http://www.cdt.org/wiretap/20041112joint.pdf>.

152. Supplemental Brief for Center for Democracy and Technology et al. at 1–4.

153. *Councilman III*, 418 F.3d at 67.

resolve complex surveillance questions. Consider also Congress's choice to incorporate electronic communications into the Wiretap Act. That choice obviated the need for courts to consider whether users can reasonably expect privacy in electronic communications, but it has also hampered courts' ability to articulate a coherent theory of how the Fourth Amendment applies to electronic communications in storage, where they are less well protected by statute.

Apart from these general observations about the problems of institutional competence arguments in cases where the legislature has chosen the rule that constrains the executive, it is worth making two additional points with respect to proactive statutes. First, I noted that Congress often confides important statutory questions in courts, but in the particular context of ECPA, Congress has limited courts' ability to interpret the relevant provisions by withholding a statutory suppression remedy. Without such a remedy, statutory challenges to executive action do not arise in criminal proceedings. No doubt the omission of a suppression remedy was motivated in part by a belief that no such remedy was warranted,¹⁵⁴ not a specific desire to foreclose judicial interpretation. The absence of a tool for courts to evaluate the SCA's terms in a criminal context, however, can hamper not only judicial evaluation, but also *legislative* evaluation. To the extent that judicial decision-making exposes an executive interpretation of the law, it facilitates public and legislative oversight. The paucity of judicial decisions under the SCA makes it unsurprising that Congress has made few significant changes to the SCA. Executive interpretations of the statute are largely shielded from view in the absence of other more direct oversight mechanisms. Although Congress has updated ECPA on nearly a dozen occasions over the last twenty-five years, most of the amendments other than the Patriot Act reflect fairly technical changes to the existing statutory framework.

3. Summary

None of this discussion is intended to suggest that broader judicial intervention on constitutional grounds is appropriate.¹⁵⁵ Rather, it is to suggest that arguments about institutional competence tend to oversimplify the surveillance law landscape. Calls for greater judicial enforcement focus

154. See *supra* note 78 (noting that Justice Department demanded omission of suppression remedy).

155. Cf. Einer R. Elhauge, *Does Interest Group Theory Justify More Intrusive Judicial Review?*, 101 YALE L.J. 31 (1991) (questioning premise that perceived defects in political process justify broader judicial review).

on executive rule-selection cases at the expense of legislative rule-selection cases. Calls for legislative supremacy, on the other hand, overlook the fact that a hands-off approach can privilege executive interpretations and substitute complex statutory questions for constitutional ones. Such arguments also ignore design issues, overlooking how one institution's decisions constrain or eliminate the possibility of another's response and how changes in institutional design could be used to *improve* the quality of legislative and judicial decisions.

B. *Second-Order Design Questions*

In this section, I seek to bring institutional design issues into play by trying to isolate those issues from normative preferences about and constitutional constraints on communications surveillance law. I then seek to identify types of design mechanisms most likely to affect the quality of decisions.

1. First-Order Preferences versus Second-Order Design Choices

The goal of institutional competence analysis is to arrive at the best institution to set first-order preferences about a particular goal—in this case (under the goal choice previously described) the best institutions to establish and police limits on executive discretion in use of surveillance tactics. Comparative institutional analysis proceeds from a position of neutrality as to what first-order preferences should be. To distinguish first-order preferences from second-order design issues, however, it is useful to get a flavor of the range of first-order preferences that the communications surveillance law framework reflects.

The Wiretap Act, for example, reflects robust limitations on executive discretion to acquire the contents of communications in transit: it restricts the *kind of information* agents can seek (to *information concerning a crime* that has been, is being, or will be committed), restricts *how much information* agents can seek (that which can be gathered within a *period of up to 30 days*, subject to renewal), and restricts the *purpose* for which agents can gather information (*preventing or investigating criminal activity*). These restrictions could obviously be implemented in a range of ways, and I refer to these choices as second-order design choices.

Consider the limitation that information gathered under the Wiretap Act must pertain to a crime. By statute, applications for surveillance of wire and oral communications require the approval of a high-level Justice Department official, and thus proceed through a centralized executive

branch review process.¹⁵⁶ In theory, the effect of such a requirement is to centralize decision-making and vest it in politically accountable officials, and perhaps even to place certain executive officials in a quasi-judicial role. By most accounts, in practice this requirement has had the effect of making the wiretap application process a fairly burdensome one for investigators.¹⁵⁷ The Wiretap Act's high-level executive review requirements no doubt contributed to the institutional evolution within the Justice Department, with the Criminal Division's Office of Enforcement Operations serving as a gatekeeper for the Title III order process. The statute, however, does not rest on executive assessment alone; it requires a judicial finding of probable cause, and at the federal level even confines that authority to district court judges (rather than magistrates).¹⁵⁸ Other aspects of the statute reflect a different allocation of responsibility. Law enforcement officials must "minimize" interception of communications not authorized to be intercepted, but judicial checks on whether they have done so are limited.¹⁵⁹ Indeed, the statute does not require judicial evaluation of whether evidence of crimes other than those set forth in the application should be disclosed, thus leaving the matter to executive discretion.¹⁶⁰ The statute does, however, require judicial evaluation of whether other-crimes evidence should be admitted into court.¹⁶¹

It should be obvious that second-order design mechanisms will often move with first-order preferences, in the sense that a preference for greater limits on executive discretion will lead to the selection of design mechanisms that rely less on executive policy and more on other institutional arrangements. Nevertheless, many different design combinations are available to meet first-order preferences. A goal of preventing unlawful executive surveillance, for example, might be achieved equally well through a statutory suppression mechanism and through the availability of a civil damages remedy against executive officials who authorize the surveillance.

156. 18 U.S.C. § 2516(1) (2006).

157. For this reason, many government officials argue that the fact that Wiretap Act applications are rarely rejected is not indicative of too-lenient judicial scrutiny. I discuss a related dynamic with respect to the Office of Intelligence Policy and Review's role in the FISA process in Bellia, *supra* note 47, at 470.

158. 18 U.S.C. § 2518(3); § 2510(9)(a).

159. *Id.* § 2518(5).

160. *Id.* § 2517(5).

161. *Id.*

2. Constitutional Constraints

It is important to explore how constitutional restrictions constrain (and do not constrain) both first-order preferences and second-order design elements. Under the Supreme Court's current interpretation of the Fourth Amendment, the invasion of a reasonable expectation of privacy constitutes a "search" and generally must be preceded by a warrant.¹⁶² Current Fourth Amendment doctrine thus acts as a backstop to normative arguments about executive discretion in surveillance law, for it prevents the executive from assigning to itself the task of determining how much evidence of criminal activity justifies conducting a "search," and whether that standard is met in a given situation. Beyond that, however, the Constitution imposes minimal constraints on first-order preferences. Nothing requires or prevents limits on executive surveillance tactics when the Fourth Amendment does not demand them.

Similarly, regarding second-order questions, the Fourth Amendment sets a floor but not a ceiling. A determination that a particular technique invades an expectation of privacy and thus constitutes a search will dictate some design rules, for it will require a mechanism for a judicial magistrate to determine before the search occurs that the search is supported by probable cause and is reasonable in scope. Where the Fourth Amendment does not compel such a determination, a legislature is free to impose procedures and allocate authority among the branches as it sees fit, and it is likewise free to impose requirements beyond those dictated by the Fourth Amendment.

If multiple options are available to meet first order preferences, and those options are sometimes independent of constitutional questions, then the possibilities for improving decisional outcomes about surveillance law tactics become more readily apparent.

C. *The Impact of Design Choices*

The previous section attempted to isolate design choices from other features of the communications surveillance law regime, including normative preferences about how much to limit executive discretion and constitutional constraints operating in the background. Here, I explore those design mechanisms most likely to affect the quality of legislative and judicial decisions about the rules governing use of surveillance techniques.

It is useful to discuss these design mechanisms with reference to an increasingly common communications surveillance tactic, involving the gathering of cell-site location information—that is, data concerning the

162. See *supra* notes 20–22 and accompanying text.

location of particular cell phone towers “hit” by a target’s phone. Data from multiple towers can be triangulated (with various degrees of precision) to identify a suspect’s physical location. The first CSLI requests to become publicly known involved applications for court orders compelling cell phone providers to collect and produce data concerning multiple towers within range of the suspect’s phone, even when no call was in progress.¹⁶³

In a series of applications, the government argued that it was entitled to acquire such data by meeting the requirements of two different statutes: the pen register and trap-and-trace device statute¹⁶⁴ and a portion of the Stored Communications Act governing disclosure of customer records.¹⁶⁵ That approach was based on the theory that information concerning a cell phone’s contact with cell towers literally fell within pen/trap statute, which covers devices used to obtain “signaling” information; although CALEA barred officials from relying solely on the pen/trap statute to obtain location information, a “hybrid” order under the pen/trap provisions and provisions of the SCA regulating access to customer records would suffice to compel production of that information.

Numerous magistrate judges accepted the government’s argument and granted the requested “hybrid” order. In 2005, however, two magistrate judges faced with such requests rejected the government’s “hybrid” approach, concluding that officials could only gather such data after obtaining a warrant based on probable cause.¹⁶⁶ A third judge followed suit,¹⁶⁷ prompting the government to seek more limited information in subsequent cases.¹⁶⁸

163. See *In re Application for Pen Register*, 396 F. Supp. 2d 747, 765 (S.D. Tex. Oct. 14, 2005) (Smith, Mag. J.).

164. 18 U.S.C. § 3121.

165. *Id.* § 2703(d).

166. See, e.g., *In re Application of the United States*, 396 F. Supp. 2d 294 (E.D.N.Y. Oct. 24, 2005) (Orenstein, Mag. J.) (rejecting government’s legal theory but noting that scope of information sought may have been more limited than that sought in prior cases); *In re Application for Pen Register*, 396 F. Supp. 2d at 747.

167. *In re Application of the United States*, 402 F. Supp. 2d 597, 605 (D. Md. Nov. 29, 2005) (Bredar, Mag. J.).

168. More specifically, the United States advanced the “hybrid” theory to justify acquiring information on single cell towers hit at the beginning, end, and (if reasonably available) during a call. Such information, the government claimed, would yield only the subject’s general location.

A majority of courts have rejected this “hybrid” approach when the government seeks to gather information prospectively. *In re Application of the United States*, 2009 WL 159187, at *6 (S.D.N.Y. Jan. 13, 2009) (McMahon, J.); *In re Application of the United States*, 497 F. Supp. 2d 301, 311 (D.P.R. July 18, 2007) (McGiverin, Mag. J.); *In re Application of the United States*, 2006 WL 2871743, at *7 (E.D. Wis. Oct. 6, 2006) (Adelman, J.); *In re Application of the United States*, 441 F. Supp. 2d 816, 827–36 (S.D. Tex. July 19, 2006) (Smith, Mag. J.); *In re Application of the United States*, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, J.); *In re*

The insights of comparative institutional analysis theorists may help to illustrate how the courts reached this result. Professor Neil Komesar's "participation-centered" framework, for example, facilitates comparisons of institutional performance by exploring, across institutions, differences among those seeking legal change in terms of the costs and benefits of institutional participation.¹⁶⁹ More specifically, in Komesar's model, the character of institutional participation varies according to the distribution of stakes in the outcome, and variations in the cost of participation—including the costs of obtaining relevant information regarding the issue in question, organizing those with an interest in the outcome, and barriers to access associated with institutional rules and procedures.¹⁷⁰

The first two judges to reject the "hybrid" theory for CSLI considered the government's applications in ordinary *ex parte* proceedings, but then sought amicus participation in opposition to the government's position. The judges essentially shifted participation costs. We can view the potential "stakeholders" in the decision as law enforcement officials on the one hand, and potential surveillance targets on the other. Potential targets are likely to have minimal knowledge about how the government interprets and applies surveillance law statutes, and an *ex parte* process obviously provides formal institutional barriers to the participation of any potential target. An *ex parte* proceeding may be unobjectionable when it involves application of a settled legal rule to a particular set of facts, rather than evaluation of executive

Application of the United States, 439 F. Supp. 2d 456, 458 (D. Md. June 24, 2006) (Bredar, Mag. J.); *In re Application of the United States*, 2006 WL 468300, at *2 (S.D.N.Y. Feb. 28, 2006) (Peck, Mag. J.); *In re Application of the United States*, 416 F. Supp. 2d 390, 397 (D. Md. Feb. 27, 2006) (Bredar, Mag. J.); *In re Application of the United States*, 415 F. Supp. 2d 211, 219 (S.D.N.Y. Feb. 15, 2006) (Feldman, Mag. J.); *In re Application of the United States*, 407 F. Supp. 2d 134, 140 (D.D.C. Jan. 6, 2006) (Facciola, J.); *In re Application of the United States*, 412 F. Supp. 2d 947, 958 (E.D. Wisc. Jan. 1, 2006) (Callahan, Mag. J.); *In re Application of the United States*, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005) (Robinson, Mag. J.); *see also In re Application of the United States*, 2006 WL 6217584 (D.D.C. Aug. 25, 2006) (Hogan, J.) (issuing a warrant under Rule 41 for disclosure of prospective cell site location information).

A minority of courts have approved applications under this theory. *In re Application of the United States*, 2009 WL 1594003 (E.D.N.Y. Feb. 26, 2009) (Garaufis, J.); *In re Application of the United States*, 632 F. Supp. 2d 202, 211 (E.D.N.Y. Nov. 26, 2008) (Garaufis, J.); *In re Application of the United States*, 622 F. Supp. 2d 411, 417 (S.D. Tex. Oct. 17, 2007) (Rosenthal, J.); *In re Application for an Order*, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007); *In re Application of the United States*, 460 F. Supp. 2d 448, 461 (S.D.N.Y. Oct. 23, 2006) (Kaplan, J.); *In re Application of the United States*, 433 F. Supp. 2d 804, 806 (S.D. Tex. Apr. 11, 2006) (Rosenthal, J.); *In re Application of the United States*, 411 F. Supp. 2d 678, 682 (W.D. La. Jan. 26, 2006) (Hornsby, Mag. J.); *In re Application of the United States*, 405 F. Supp. 2d 435, 450 (S.D.N.Y. Dec. 20, 2005) (Gorenstein, Mag. J.).

169. NEIL KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 8 (1994).

170. *Id.*

rule-selection in the first instance. By soliciting amicus participation in an executive rule-selection case, the judges effectively adjusted participation costs in an area of great legal uncertainty.

It bears reminder that the purpose of the participation-centered model I discuss here is comparative: the point is not that shifting participation costs makes it more likely that courts will reach the right substantive result. Rather, the shift is important to the extent that, in adjusting the stakes and costs within one or more institutions, it changes the benchmark against which to measure the performance of other institutions (in this case, the legislature).

In the next Part, I further develop this approach to design choice.

III. IMPROVING DESIGN CHOICES IN COMMUNICATIONS SURVEILLANCE LAW

In Part II, I suggested that institutional competence claims about whether courts or legislatures are best suited to limit executive discretion in surveillance tactics envision a binary institutional choice rather than an iterative process, and take institutional design as a given. I then explored, with the help of the cell-site dispute, how design choices might matter in this context. In particular, I focused on choices that alter the costs and benefits of institutional participation, whether in courts or legislatures.

In this Part, I elaborate upon those observations. My analysis proceeds from the premise that a prevailing surveillance law regime might differ from that which would match first-order policy preferences (whether courts, legislatures, or both arrive at those preferences). I first identify features that alter the cost and benefit of institutional participation in surveillance law decisions; I then apply some of these features in the context of two of the institutional patterns identified in Part I of this Essay.

As will become clear, the features I discuss all serve in various ways to check executive discretion in the use of surveillance law tactics, and are thus vulnerable to the charge that they simply mask a normative preference for greater privacy. The executive-checking function, however, simply flows from my assumption—which I believe to be uncontroversial—that the role of a surveillance law regime is to cabin executive discretion. Moreover, it is important to note that I do not urge application of all of these measures across any particular range of surveillance law questions. Rather, my claim is that courts and legislatures should consider adopting certain measures for certain high-stakes decisions, particularly those involving courts' review of newly selected surveillance rules and those involving legislatures' adoption of proactive statutes.

A. *Theory: Shifting Stakes and Costs*

In this Section, I consider some of the design tools available to shift the stakes and costs of participants in legislative and judicial decisions about surveillance tactics.

Stakes. As to both judicial and legislative decisions constraining communications surveillance tactics, law enforcement interests have high stakes. Congressional action within the legislative process will generate nationwide rules authorizing or constraining law enforcement techniques. The stakes might seem lower with respect to any individual judicial decision about the legality of a surveillance technique, except that decisions regarding large-scale providers (such as America Online or Yahoo!) can effectively nationalize surveillance rules as well.¹⁷¹ In short, whether in legislative or judicial fora, law enforcement interests have strong incentives to press for expansive interpretations of surveillance law powers.

Although law enforcement stakes are high in either context, two mechanisms, one legislative and one judicial, can operate to shift those stakes. First, a “sunset” mechanism of the sort adopted in the USA Patriot Act further raises the stakes of law enforcement participation in the legislative process, because law enforcement interests face the potential loss of existing surveillance powers rather than merely an absence of new powers. Second, statutes that restrain both law enforcement conduct and private conduct may temper law enforcement stakes in achieving a narrow construction of the statutory provisions, because in eliminating restrictions on their own conduct, law enforcement officials also eliminate their ability to prosecute private parties for similar conduct.¹⁷²

171. The nationalizing effect of decisions regarding Internet service providers should not, however, be overstated. Before Congress passed the USA Patriot Act, the SCA required investigators seeking to compel a provider to disclose communications to obtain the relevant order in the district in which the provider was located. Thus, for example, requests for America Online to disclose communications would be made to the Eastern District of Virginia, no matter where the investigation was proceeding. In the Patriot Act, Congress authorized courts of the jurisdiction in which the investigation was proceeding to grant such orders. See CCIPS MANUAL, *supra* note 117, at 134 (noting that the SCA permits a judge to compel production of records located in another district); Bellia, *supra* note 23, at 1454 (describing change). The change raises the possibility that requests directed to the same provider will be subject to different standards, depending on the law of the investigating jurisdiction.

172. Professor Paul Ohm calls such statutes “parallel-effect” statutes. See Paul K. Ohm, *Parallel-Effect Statutes and E-Mail “Warrants”: Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599 (2004); Bellia, *supra* note 127, at 1341 (discussing government’s complex incentives in this context). For a related argument about statutes containing both civil and criminal penalties, see Lawrence M. Solan, *Statutory Inflation and Institutional Choice*, 44 WM. & MARY L. REV. 2209 (2003).

In both the legislative process and the judicial process, the benefits to potential targets of limitations on executive discretion in surveillance law are likely to be widely dispersed. Any actual target is completely outside of the legislative process, but may have high stakes in the judicial process. These stakes, however, are largely a function of design. Under the Wiretap Act, for example, a surveillance target is entitled to suppression of evidence for purely statutory violations in cases involving acquisition of wire and oral communications, but not in cases involving acquisition of electronic communications.¹⁷³ No statutory suppression remedy is available under the SCA.¹⁷⁴

Finally, communications providers add another layer of complexity to the analysis. In the legislative process and in the judicial process, providers are likely to have an incentive to advocate limits on executive discretion in surveillance law because broader use of surveillance techniques will be costly to providers. Of course, cost-shifting statutes, such as the provisions of CALEA requiring the government to reimburse carriers for some costs of updating equipment to facilitate surveillance requests,¹⁷⁵ as well as other assistance provisions in surveillance law statutes themselves,¹⁷⁶ may limit providers' incentives to seek restraints on executive discretion in surveillance law. Indeed, although government officials have reportedly used hundreds-of-thousands of national security letters to seek information from various record holders,¹⁷⁷ and presumably a sizable number of these letters were issued to communications providers under the SCA's NSL provisions, there have been only a handful of publicly reported instances of providers challenging NSLs.¹⁷⁸ On the other hand, a provider's incentives may be complicated by the anticipated backlash if it cooperates, or the anticipated praise if it refuses to cooperate, with a request that its subscribers or the public perceive to be unreasonable.¹⁷⁹

173. 18 U.S.C. §§ 2515, 2518(10) (2006).

174. *Id.* § 2708 (providing that civil remedies are exclusive nonconstitutional remedies for violations of SCA).

175. *See* 47 U.S.C. § 1008 (2006).

176. *See, e.g.*, 18 U.S.C. § 2706(a) (requiring governmental entity to reimburse provider for reasonably necessary costs directly incurred in "searching for, assembling, reproducing, or otherwise providing" requested communications or records).

177. *See, e.g.*, OFFICE OF THE INSPECTOR GENERAL, U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE in 2006, at 9 (2008).

178. *See, e.g.*, *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005); *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

179. For example, Twitter successfully challenged, to much public approbation, the secrecy attached to a court order demanding that it provide information regarding the accounts of

Information costs. Both in the legislative process and in the judicial process, law enforcement interests will have full access to all information about executive interpretations of surveillance law rules, the frequency with which certain tactics are deployed, and how effective those statutes are. In both the legislative process and the judicial process, information costs of actual and potential targets—as well as communications providers—are much higher.

Consider first the possible sources of information about executive interpretations of surveillance law rules. Such interpretations can emerge in the context of individual cases, but of course, whether they do so depends in part on the likelihood that a target will challenge use of the surveillance tactic—which in turn depends on the target's stake in the outcome of the case. As we have seen, the absence of a statutory suppression mechanism, as for electronic communications under the Wiretap Act and the SCA, will tend to limit courts' opportunity to construe the relevant statutes. The FISA regime yields a similar observation. Although FISA contains a suppression mechanism, a surveillance target typically only receives notice of the surveillance when the government intends to introduce FISA-derived information in a judicial or other proceeding.¹⁸⁰ Although there have been more than 28,000 FISA applications and renewals granted since 1979, challenges to introduction of FISA-derived evidence or demands for disclosure of FISA-derived evidence have been raised in approximately thirty-five cases,¹⁸¹ and none of these challenges has been successful.¹⁸² Questions about the legality of FISA surveillance also have arisen in a handful of other cases not directly involving suppression or disclosure motions, with only one court concluding that FISA surveillance was unlawful.¹⁸³ Because questions concerning the legality of particular searches

particular subscribers. *See* Noam Cohen, *Twitter Shines a Spotlight on Secret F.B.I. Subpoenas*, N.Y. TIMES, Jan. 9, 2011, at B3.

180. *See* 50 U.S.C. § 1806(c)–(d) (2006). FISA also generally requires notice when the Attorney General approves electronic surveillance on an emergency basis and a request for a court order is subsequently denied. *See id.* § 1806(j).

181. The number in the text reflects cases published in the national reporter system or available on Westlaw or Lexis. It includes eighteen cases in which a court of appeals affirmed denial of a suppression motion and/or a motion seeking disclosure of FISA-derived evidence and seventeen cases decided at the district court level and apparently not appealed. The figure does not include purely procedural dispositions, such as a determination that a party lacks standing to contest the legality of FISA's use or that a challenge to FISA's use is not properly brought at a particular stage of the case.

182. Although suppression is also quite rare in the Title III context, the sheer number of suppression motions under Title III makes tabulation and comparison impossible.

183. Such cases might involve, for example, a civil suit, a request by the government for a declaratory judgment concerning the legality of the surveillance, or a challenge referred to a U.S. district court concerning evidence sought to be used in a foreign proceeding. A district

arise relatively infrequently, judicial articulation of legal norms under FISA is quite rare. We can glean some information about executive interpretation of FISA from episodic reporting on particular crises.¹⁸⁴ In general, however, the information costs for those seeking to impose limits on executive discretion, whether in courts or in the legislature, are high.

Consider next the possible sources of information about how widely the executive uses certain surveillance law tactics. When no statute compels the release of such information, outsiders must rely on information the government voluntarily releases or the fruits of Freedom of Information Act litigation.

Certain design mechanisms can of course shift these information costs. I have elsewhere discussed the “information structure” of the foreign intelligence surveillance scheme—that is, the institutional mechanisms designed to generate the information necessary for evaluation of how the executive and the FISC have implemented the foreign intelligence surveillance framework.¹⁸⁵ Post-surveillance review is sufficiently rare that it does not provide much informational value, but Congress has also imposed certain public and inter-branch reporting requirements on the executive.¹⁸⁶ More specifically, FISA requires the Attorney General to transmit to the Administrative Office of United States Courts and to Congress reports setting forth “the total number of applications made for orders and extensions of orders approving electronic surveillance” under FISA and “the total number of such orders and extensions either granted, modified, or denied.”¹⁸⁷ The statute also requires the Attorney General to “fully inform” the congressional intelligence committees “concerning all electronic surveillance” under FISA.¹⁸⁸ In addition, as enacted FISA required the intelligence committees, for five years after FISA’s enactment, to report to their respective chambers concerning implementation of the statute, including whether FISA should be amended, repealed, or permitted

court declared FISA surveillance unlawful in *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007), but the ruling was vacated on procedural grounds. *Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010).

184. See GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 11–15 (2001) available at <http://www.gao.gov/products/GAO-01-780>; ATTORNEY GENERAL’S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION, FINAL REPORT 707–52 (2000), available at <http://www.usdoj.gov/ag/readingroom/bellows.htm>.

185. See generally Bellia, *supra* note 47.

186. See S. REP. NO. 95-604, pt. 1, at 60 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3961–62; S. REP. NO. 95-701, at 66–67 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 4035–36.

187. 50 U.S.C. § 1807 (2006).

188. *Id.* § 1808(a).

to continue in effect.¹⁸⁹ All of these reports were made public.¹⁹⁰ At least in theory, these sorts of requirements lower information costs by allowing both for the evaluation of FISA's privacy implications and for the evaluation of the executive's and the FISC's fidelity to congressional intent. (As discussed below, although FISA as enacted reflected a carefully designed information structure, Congress has paid far less attention to such measures as the statute has evolved.)

Institutional barriers and other organizational costs. Finally, I briefly examine institutional barriers and other organizational costs reflected in the surveillance law regime. Law enforcement interests face minimal institutional barriers in courts or the legislature. When seeking an *ex parte* application to use a particular surveillance tactic, law enforcement will be the sole party represented, and the government will always be available to defend a suppression motion. There will of course be some cases where interpretations of surveillance law statutes will arise in purely civil disputes to which the government is not a party. In such cases, courts' interpretations of the statutes will bear upon the scope of agents' authority. Because courts appear to readily accept amicus participation by the United States in such cases, however, institutional barriers remain low.

For actual and potential surveillance targets, the institutional barriers and other organization costs are much more significant. In the legislative process, dispersed stakes come with higher organization costs, although the growth in information privacy groups (and the ease with which they can reach members via the Internet) may reduce such costs. Potential targets will not be represented in *ex parte* proceedings involving applications for use of surveillance tactics unless, as in the cell site cases, courts invite *amici* to participate.

Finally, communications providers are sufficiently organized that they will face relatively low costs in the legislative process. When providers are not forced to bear the cost of surveillance tactics, however, they have limited incentives to oppose government demands for more surveillance power. In the judicial process, a provider that receives a surveillance order will have standing to seek to quash the application, and so there are no formal institutional barriers to its participation. Yet unless a request is particularly burdensome, or the provider fears a backlash if its compliance

189. *Id.* § 1808(b).

190. See S. REP. NO. 98-660 (1984); H.R. REP. NO. 98-738 (1984); S. REP. NO. 97-691 (1982); H.R. REP. NO. 97-974 (1982); S. REP. NO. 97-280 (1981); H.R. REP. NO. 97-318 (1981); S. REP. NO. 96-117 (1980); H.R. REP. NO. 96-1466 (1980); S. REP. NO. 96-379 (1979); H.R. REP. NO. 96-558 (1979).

with government investigators becomes public, its incentives to challenge government surveillance tactics may be limited.

B. Application: Executive Rule-Selection and Proactive Statutes

The previous section explored the stakes and costs of various parties interested in how courts and legislatures should check executive discretion as to the use of surveillance law techniques. I identified a number of ways in which design changes could shift the stakes or costs involved.

In this section, I attempt to make the analysis more concrete by returning to some of the institutional patterns identified in Part I. (I leave aside “reactive” legislative rules.) Although I have identified a number of design changes that could shift the stakes and costs of participants in the legislative and judicial processes, I have not suggested that any or all of these shifts would be appropriate in particular cases. Here, I attempt to isolate some patterns in which the costs of legislative or judicial error are particularly high, and where shifting the levels of institutional participation may therefore be helpful.

1. Judicial Decisions on Executive Rule-Selection

The institutional patterns of Part I illustrated that scholars often understate the judicial role in the surveillance law landscape. Because Congress reacts to judicial decisions, whether to implement the decision or to supplement weak procedural rules the court prescribes, the judicial decision fades into the background. As I argued in Part I, however, even where a statute immediately follows a judicial decision, the initial decision likely determines whether there will be strong or weak checks on the executive’s use of a particular surveillance tactic.¹⁹¹

It follows that judicial responses to instances of *executive rule-selection* represent the most important point of judicial decision, for they likely set the path of future legislative action. This fact counsels in favor of courts seeking the fullest possible participation when a new question about executive rule-selection arises. The magistrate judges who invited amicus participation at the *ex parte* application stage had precisely this instinct. Amicus participation not only reduces the information costs and lowers participation barriers for potential targets (represented by privacy groups), it also raises the government’s participation costs, and may thereby cause law enforcement officials to gauge more precisely the need for the tactic

191. See *supra* Part I.C.2.a.

involved. In late 2006, for example, the government filed an application in the Southern District of New York seeking disclosure of the contents of text messages logged with a service provider. When the court notified the government that it intended to invite amicus participation and request briefing, the government immediately withdrew the application.¹⁹²

2. Proactive Statutes

Recall the two categories of “proactive” statutes in Part I: “modernizing” statutes, in which Congress makes a judgment about the state of technology and metes out roles for executive and judicial participation in the process of deciding when the substantive standards are met; and “crisis response” statutes, in which Congress responds to perceived intelligence or investigative failures by filling gaps. Each pattern presents a serious risk that a mismatch will develop between the statute and first-order policy preferences. In the case of a modernizing statute, we can assume that first-order preferences remain relatively constant, but changes in technology alter the effective scope of the surveillance tactics the statute allows. In the case of a crisis response statute, we can posit that the statute matches preferences when passed, but that a mismatch occurs when preferences return to pre-crisis levels. How might design choices help Congress or the courts correct a mismatch?

a. Crisis Response Statutes

The design possibilities on the legislative side are best illustrated by the model of the crisis-response statute. I earlier described the gradual expansion of FISA’s scope as a series of responses to perceived investigative failures.¹⁹³ FISA initially covered electronic surveillance. Congress later added provisions authorizing FISC orders for physical searches, the use of pen registers and trap and trace devices, and production of business records.¹⁹⁴ In the wake of the September 11 attacks, Congress loosened the necessary showing of purpose¹⁹⁵ and dramatically expanded the category of items that could be compelled from third parties to encompass tangible things rather than business records.¹⁹⁶

192. E-mail from Kevin Bankston, Senior Staff Attorney, Electronic Frontier Foundation to author (Feb. 13, 2007) (on file with author).

193. See *supra* notes 86–93 and accompanying text.

194. See *supra* notes 87–89 and accompanying text.

195. See Bellia, *supra* note 47, at 452–56; *supra* notes 131–39 and accompanying text.

196. See Bellia, *supra* note 47, at 447.

For purposes of the discussion, we can assume that short-term changes in first-order policy preferences facilitated at least some of these statutory changes. The question is whether Congress (or the courts) will adjust the provisions if preferences shift back to pre-crisis levels. The stakeholders in the ultimate decision are law enforcement officials, actual (known and unknown) and potential surveillance targets, and communications providers who must execute surveillance orders. Law enforcement officials will have the lowest information-gathering and organization costs; they have access to all relevant information on the use of surveillance tactics as well as routinized contacts with the congressional committees most likely to influence the decisional outcomes here. Although communications providers are sufficiently well organized that they may not face high organization costs, they are unlikely to have substantial information on the scope and effectiveness of surveillance tactics, outside of cases in which they have been specifically involved. Since actual targets are not known in advance, the information and organization costs are insurmountable. The matter is left to potential targets—i.e., the public. Even assuming that the increasing concentration of information privacy groups will make organization costs more manageable, the information costs remain high.

Note, however, how design mechanisms can shift the dynamics. A sunset mechanism such as that included in the USA Patriot Act substantially shifts the parties' stakes by making a resort to the status quo ante a consequence of inaction.

Merely adding a sunset mechanism, however, does not necessarily alter the information costs the parties face. Here, a robust "information structure" along the lines I described above becomes critical.¹⁹⁷ As I have argued elsewhere, however, although FISA's original information structure was a careful counterweight to the absence of broad post-surveillance review on the structure, until recently Congress has entirely neglected that information structure, despite the dramatic expansions in statutory scope.¹⁹⁸ Even recent changes that on the surface are designed to expand the executive's reporting requirements have been narrowly interpreted to permit classified reporting.

b. Modernizing Statutes

The design possibilities on the judicial side are best illustrated by the example of modernizing statutes. Depending on the statutory scheme, judicial intervention could take one of three forms: (1) *ex parte* review of an application for surveillance; (2) review of a communication provider's

197. See *supra* notes 185–90 and accompanying text.

198. Bellia, *supra* note 47, at 462–67.

objection to an order (presumably in the context of a motion to quash); (3) or some form of *ex post* review.

I have already discussed the importance of amicus participation at the *ex parte* application stage when a court assesses executive rule-selection.¹⁹⁹ The arguments there fully support amicus participation in evaluation of an application under a modernizing statute as well. When technology shifts to the point where mapping a statute onto new technology becomes difficult, the executive's interpretation of the statute functionally becomes more like an a legal interpretation outside of the confines of a statute. Interpreting the statute narrowly, moreover, tends to privilege the executive's interpretation of the law, just as a cautious approach to the Fourth Amendment does in the case of executive rule selection.

Finally, the absence of *ex post* enforcement mechanisms will defeat courts' ability to resolve a case in the situation when the most stakeholders are likely to be represented and when the stakes are highest. Indeed, we can identify several current surveillance statutes as to which the law is underdeveloped, in all likelihood because of the absence of an *ex post* enforcement mechanism.²⁰⁰ As noted earlier, the absence of a suppression mechanism not only affects courts' ability to check executive discretion in use of surveillance techniques, it can eventually affect legislatures' ability to do so as well, by eliminating public scrutiny of executive interpretations of the law.²⁰¹

IV. CONCLUSION

Explaining the limited nature of judicial regulation of surveillance tactics in the post-*Katz* era is perhaps easier than it seems: judicial silence in communications surveillance cases is a function of context, and sometimes masks a powerful behind-the-scenes judicial rule, but other times reflects the difficulty of dislodging executive powers in the wake of technological shifts or changing views of a recent crisis. The harder puzzle for surveillance law scholars is how to sort out the appropriate legislative and judicial roles. Second-order design techniques play a thus-far

199. See *supra* notes 191–92 and accompanying text.

200. Neither the pen register and trap-and-trace device statute nor the Stored Communications Act contains a statutory suppression remedy. For related arguments about how suppression remedies would improve interpretation of the SCA, see Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 807 (2003); Freiwald, *Online Surveillance*, *supra* note 9, at 63.

201. See *supra* note 154 and accompanying text.

underappreciated role in influencing the quality of decisional outcomes in such controversies.