

A SECOND-ORDER THEORY OF COMMUNICATIONS SURVEILLANCE LAW

Patricia L. Bellia*

Communications surveillance law is largely statutory. That fact might seem puzzling, for we would expect the Supreme Court’s decision in Katz v. United States to herald continued constitutionally-based regulation of surveillance law tactics. The scholarly literature offers divergent positive and normative perspectives on courts’ relative post-Katz silence on the constitutionality of communications surveillance tactics: some scholars argue that courts are overly deferential to executive and legislative decisions about surveillance tactics, while others suggest that current law reflects a sensible allocation of legislative and judicial roles in light of the comparative competence of legislatures and courts to address how the law should treat rapidly evolving technologies.

These inquiries into questions of institutional competence add an important perspective to the study of communications surveillance law—but, I argue, one that is ultimately incomplete. Such inquiries tend to take institutional structure as a given, thereby predicting the quality of decisions while bracketing questions of institutional design that could themselves influence the quality of decisions. In short, institutional competence analyses of communications surveillance law seek to choose the institutional decision-maker best suited to arrive at first-order policy preferences, but they neither take account of nor generate constraints on the second-order design choices available to implement those preferences. This article seeks to bring second-order design questions to the forefront of the surveillance law debate and to provide a framework for considering these questions.

INTRODUCTION	2
I. INSTITUTIONAL PATTERNS IN COMMUNICATIONS SURVEILLANCE LAW	8
A. <i>Four Surveillance Law Patterns</i>	9
1. <i>Executive Rule-Selection</i>	10
2. <i>Legislative Rule-Selection</i>	12
a. <i>Reactive statutes</i>	12
b. <i>Proactive statutes</i>	16
B. <i>Understanding the Judicial Landscape</i>	23
1. <i>Executive Rule-Selection</i>	25
2. <i>Legislative Rule-Selection</i>	27
a. <i>Reactive statutes</i>	27
b. <i>Proactive Statutes</i>	28
3. <i>Summary</i>	37
II. FROM FIRST-ORDER TO SECOND-ORDER QUESTIONS IN SURVEILLANCE LAW	37
A. <i>Comparative Institutional Competence</i>	38
1. <i>Executive Rule-Selection</i>	40
2. <i>Legislative Rule-Selection</i>	41

* Visiting Professor, University of Virginia School of Law; John Cardinal O’Hara, C.S.C. Associate Professor of Law, Notre Dame Law School. A.B. Harvard College, J.D. Yale Law School. I thank Orin Kerr, Peter Swire, and participants at a faculty workshop at the George Washington University School of Law for helpful comments.

3. Summary	45
B. Second-Order Design Questions.....	45
1. First-Order Preferences versus Second-Order Design Choices	46
2. Constitutional Constraints	48
C. The Impact of Design Choices	49
III. IMPROVING DESIGN CHOICES IN COMMUNICATIONS SURVEILLANCE LAW	52
A. Theory: Shifting Stakes and Costs	53
B. Application: Executive Rule-Selection and Proactive Statutes	59
1. Judicial Decisions on Executive Rule-Selection	60
2. Proactive Statutes	61
a. Crisis Response Statutes	61
b. Modernizing Statutes	63
IV. CONCLUSION.....	64

INTRODUCTION

The law of communications surveillance presents a puzzle.¹ In 1967, in *Katz v. United States*, the Supreme Court held that use of an electronic device to overhear a suspect’s conversation is a “search” for purposes of the Fourth Amendment and therefore cannot proceed without a warrant.² In so holding, the *Katz* Court shifted the focus of the Fourth Amendment away from protecting property toward protecting privacy. The provision, the Court reasoned, “protects people—and not simply ‘areas’—against unreasonable searches and seizures,”³ and thus guards against invasion of “the privacy upon which [a target] justifiably relie[s].”⁴ Whatever *Katz* might mean for other areas of

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 of 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 transactional 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 which 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 (2005); Christopher Slobogin, *Technology-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards*, 10 *HARV. J. L. & TECH.* 383, 387-88 (1997).

² 389 U.S. 347 (1967).

³ *Id.* at 353.

⁴ *Id.*

Fourth Amendment jurisprudence, one might expect that the case would herald continued judicial regulation of communications surveillance activities. In fact, since *Katz*, constitutionally based judicial regulation of communications surveillance tactics has been quite limited. In 1972, in *United States v. United States District Court of the Eastern District of Michigan* (commonly known as the *Keith* case⁵), 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.⁶ The two major statutes regulating government surveillance of communications in the wake of *Katz* and *Keith*—for criminal investigations, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III” or the “Wiretap Act”),⁷ and for foreign intelligence investigations, the Foreign Intelligence Surveillance Act of 1978 (“FISA”)⁸—have withstood all constitutional challenges.⁹

In addition, until recently, courts were entirely silent on the constitutionality of a 1986 statute that, although ostensibly designed to protect the privacy of stored wire and

⁵ 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.

⁶ 407 U.S. 297, 320 (1972).

⁷ Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 200, 214 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000 & Supp. IV 2004)).

⁸ Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 1783 (1978) (codified as amended at 50 U.S.C.A. §§ 1801-1862 (West 2000 & Supp. 2007)).

⁹ More precisely, both statutes have withstood a range of facial and as-applied Fourth Amendment challenges. For discussion of the Wiretap Act cases, see 1 JAMES G. CARR & PATRICIA L. BELLIA, *THE LAW OF ELECTRONIC SURVEILLANCE* §§ 2:45-2:56, 2:59-2:60. For a discussion of the FISA cases, see 2 *id.* §§ 9:10-9:12. Both statutes have also withstood various First, Fifth, and Sixth Amendment challenges to provisions addressing government (as distinct from private) surveillance activities. *Cf. Bartnicki v. Vopper*, 532 U.S. 514 (2001) (holding that First Amendment precluded application of Wiretap Act’s disclosure prohibition, 18 U.S.C. § 2511(1)(c), to media entity that received and broadcast excerpts from a conversation unlawfully recorded by a private party).

electronic communications,¹⁰ allows government officials to obtain such communications on standards lower than those in the Wiretap Act and in many cases without a warrant.¹¹ In July 2006, a district court enjoined the government from relying on those provisions; the case, *Warshak v. United States*, is now pending before the United States Court of Appeals for the Sixth Circuit.¹² Although a handful of courts have held that communications surveillance activities undertaken outside the confines of existing surveillance statutes violate the Fourth Amendment,¹³ until *Warshak* no court had upheld a constitutional challenge to conduct undertaken pursuant to a federal statute governing criminal or national security surveillance activities.¹⁴ Moreover, even courts showing much sympathy for claims that certain techniques invade privacy have gone to great

¹⁰ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201-202, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C.A. §§ 2701-2709, 2711-2712 (West 2000 & Supp. 2007)).

¹¹ See 18 U.S.C. § 2703 (2000). I discuss the interpretation of the relevant provisions below. See *infra* notes 84-94 and accompanying text.

¹² Order Granting in Part and Denying in Part Plaintiff's Motion for TRO, *Warshak v. United States*, No. 1:06-cv-357, 2006 U.S. Dist. LEXIS 50076 (S.D. Ohio July 21, 2006).

¹³ In August 2006, a district court held that the Terrorist Surveillance Program conducted by the National Security Agency violates the First and Fourth Amendments and separation of powers. *Am. Civil Liberties Union v. Nat'l Security Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006). In addition, two military court decisions, *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), and *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996), have held that government agents' acquisition of stored electronic communications without a warrant violates the Fourth Amendment. Finally, after assuming or holding that silent video surveillance constitutes a Fourth Amendment search, courts have required government agents using that technique to satisfy Title III-like requirements. 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, 882-884 (7th Cir. 1984).

¹⁴ The discussion in the text excludes a September 2004 district court decision holding that a provision allowing federal officials to issue a "national security letter" to a communications service provider for disclosure of certain communications records violated the First and Fourth Amendments. *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). I exclude the case because the district court never questioned the Government's substantive authority to issue national security letters for disclosure of communications records. Rather, it held that the provision granting that power could not be severed from a constitutionally problematic procedural provision barring the recipient of an NSL from ever disclosing existence of the NSL, even to counsel for the purpose of complying with the letter's terms. See also *infra* note 38.

lengths to establish statutory rather than constitutional bases for their decisions.¹⁵

Although courts' preference for avoiding constitutional questions wherever possible might explain those holdings, it cannot explain the surprisingly limited discussion of how constitutional concerns might constrain courts' interpretation of the statutes.¹⁶

What accounts for courts' relative post-*Katz* silence on the application Fourth Amendment to communications surveillance tactics? The scholarly literature offers divergent positive and normative perspectives. Most scholars see the problem as one of judicial abdication: Courts are overly deferential to executive and legislative decisions about surveillance tactics and must treat such decisions far more skeptically if they are to fulfill the role that the Constitution assigns to them.¹⁷ In other words, courts and the Fourth Amendment can and should play a major role in regulating communications surveillance tactics.¹⁸

On the other side of the debate, some scholars see a much narrower role for courts and the Constitution. Most prominent in this group is the work of Professor Orin Kerr.

In a provocative article entitled *The Fourth Amendment and New Technologies:*

Constitutional Myths and the Case for Caution, Professor Kerr argues that the doctrinal,

¹⁵ In this regard, consider the May 2002 decision of the Foreign Intelligence Surveillance Court restricting consultations within the Justice Department between criminal and counterintelligence officials in FISA investigations, *see infra* notes 100-105 and accompanying text; and a series of decisions concerning the standard under which agents may gather real-time data concerning the particular cell phone towers “hit” by a cell phone—data that can be “triangulated” to discern the location of the targeted cell phone, *see infra* notes 126-129 and accompanying text.

¹⁶ Of the cell-site cases cited in note 129, the most significant discussion of the constitutional avoidance canon appears in *In re United States*, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006).

¹⁷ *See, e.g.*, Susan Herman, *The USA Patriot Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67 (2006); Susan Friewald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004); Tracey Maclin, *Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51 (2002); Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. (2002) 1303; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1296 (2004).

¹⁸ *See, e.g.*, Herman, *supra* note 17, at 118-32; Simmons, *supra* note 17, at 1357; Slobogin, *Transaction Surveillance*, *supra* note 1, at 167-82, 189.

historical, and functional predicates for constitutionally based judicial regulation of communications surveillance tactics (and of new search technologies more generally) are lacking.¹⁹ Doctrinally, *Katz* and other decisions are best understood as loosening, but not jettisoning, a property-based conception of the Fourth Amendment.²⁰ Historically, regulation of new search technologies has been constitutional in theory but primarily statutory in fact.²¹ And functionally, courts are far less competent than legislatures to tackle the problem of regulating rapidly evolving technologies.²² In Professor Kerr's view, the post-*Katz* puzzle of judicial silence on the constitutionality of new surveillance technologies simply reflects the comparative competence of courts and legislatures in this area, and courts should continue to take a hands-off approach. Recent work by Professor Steven Penney echoes this perspective.²³

Each of these accounts implicitly or explicitly frames the normative question as one of institutional competence. All agree that the role of a surveillance law regime is to impose some controls on executive discretion. The question is not what those controls should be, but who should set them—courts through application of the Constitution, or legislatures through statutes and the oversight process.

These inquiries into questions of institutional competence add an important perspective to the study of communications surveillance law—but, I argue, one that is ultimately incomplete. First, such inquiries tend to take institutional structure as a given, thereby predicting the quality of decisions while bracketing questions of institutional

¹⁹ Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

²⁰ *Id.* at 815-27.

²¹ *Id.* at 839-57.

²² *Id.* at 857-87.

²³ See Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach* (unpublished manuscript, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=906874).

design that could themselves influence the quality of decisions. Second, and relatedly, such inquiries tend to overlook the sequential or iterative nature of decision-making, including the degree to which judicial decisions shape legislative responses, the degree to which legislative responses expand or limit the role of courts, and so on.

In short, institutional competence analyses of communications surveillance law seek to choose the institutional decision-maker best suited to arrive at “first-order” policy preferences, but they neither take account of nor generate constraints on the “second-order” design choices available to implement those preferences. Inattention to design choices, however, can create or exacerbate a gap between the communications surveillance regime that would match first-order policy preferences and the regime that is likely to prevail. This Article 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 Article proceeds as follows. Part I seeks to clarify the role that courts have played in generating communications surveillance rules. It does so by identifying the recurring institutional patterns that give rise to surveillance law challenges. Analyzing judicial decisions in light of those patterns shows that advocates of legislative supremacy in structuring a surveillance law regime dramatically understate the role of courts.

Part II turns to second-order design questions. It begins by exploring the institutional competence arguments and showing how viewing a judicial or legislative decision in isolation rather than in sequence can oversimplify those arguments by failing to account for how design choices affect decisional quality. It then attempts to disentangle second-order design choices from first-order policy preferences and shows

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: features that alter the participants' *stake* in institutional processes, features that generate and limit *information* available to decision-makers and others, and 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 that which would match first-order preferences (however generated). Part IV concludes.

I. INSTITUTIONAL PATTERNS IN COMMUNICATIONS SURVEILLANCE LAW

By all indications, communications surveillance is becoming an increasingly important weapon in government efforts to detect and thwart criminal and terrorist activities. Between 2000 and 2005, surveillance applications under the Wiretap Act increased by 48 percent²⁴ and surveillance applications under FISA increased by more than 100 percent.²⁵ These statistics of course dramatically undercount communications surveillance activities, including those authorized by courts under statutes requiring no reporting (such as the Stored Communications Act) and those undertaken without judicial authorization (as in connection with the National Security Agency's terrorist surveillance program).

²⁴ See ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 2005 WIRETAP REPORT tbl. 7, available at <http://www.uscourts.gov/wiretap05/Table72005.pdf>.

²⁵ Letter from John Ashcroft, Attorney General, U.S. Dep't of Justice, to L. Ralph Mecham, Director, Administrative Office of United States Courts (Apr. 27, 2001), at <http://www.usdoj.gov/oipr/readingroom/2000fisa-ltr.pdf>; Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, U.S. Dep't of Justice, to L. Ralph Mecham, Director, Administrative Office of United States Courts (Apr. 28, 2006), at <http://www.usdoj.gov/oipr/readingroom/2005fisa-ltr.pdf>. FISA statistics do not differentiate between applications for electronic surveillance orders and applications for physical search orders; the figure in the text assumes that such orders would have increased in roughly equal proportion.

Against this backdrop, questions of how to reconcile privacy and law enforcement interests—and, more specifically, what limits the law should impose (if any) on executive discretion in this area—take on paramount importance. 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 most of the statutes have not been subject to serious challenge in the post-*Katz* era. 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 in this area 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 in this area.

To facilitate discussion of these competing views, here I introduce four recurring institutional patterns in which constitutional questions about the use of surveillance tactics arise. My purpose is two-fold. First, viewing surveillance law questions through the lens of these four institutional patterns helps to clarify the landscape of judicial decision-making that one must explain. Second, the patterns provide a more concrete setting within which to consider the competing claims about institutional competence, and thus facilitate evaluation of those claims.

A. *Four Surveillance Law Patterns*

We can identify at least four institutional patterns giving rise to constitutional questions about the use of surveillance tactics. I first distinguish between disputes

involving *executive* rule-selection and *legislative* rule-selection. Within the latter category, I explore both *reactive* statutes—that is, statutes that implement or otherwise respond to judicial decisions about the constitutionality of executive conduct—and *proactive* statutes—that is, statutes that respond to executive conduct in the absence of a specific judicial decision. Among proactive statutes, it is also helpful to differentiate between *modernizing* statutes that respond to technological changes, and *crisis response* statutes that seek to fill perceived gaps in investigative or intelligence authorities.

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. I intend these patterns to serve as a useful analytic tool rather than precise descriptors of the surveillance law landscape. 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 the question 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*

First, a Fourth Amendment question arises when 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 the executive so claims), and 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 successfully challenge the tactic 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 certain wiretapping and eavesdropping activities until the Court's decisions in *Katz* (and *Berger v. New York*²⁶ in the immediately preceding term);²⁷ 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 in *Smith v. Maryland* held the Fourth Amendment inapplicable to that practice;²⁸ the use of covert video surveillance tactics in the absence of specific legislative authorization;²⁹ and the implementation of the NSA's terrorist surveillance program outside of the requirements of FISA.³⁰

²⁶ 388 U.S. 41 (1967).

²⁷ This example is complicated, because the Communications Act of 1934 provided that “no 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, 48 Stat. 1064, 1100 (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. For discussion of the pre-Title III history of wiretapping among state and federal officials, see Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 28-31 (2004).

²⁸ 442 U.S. 735 (1979).

²⁹ See *supra* note 13; *infra* notes 79-80 and accompanying text.

³⁰ *Am. Civil Liberties Union v. Nat'l Security Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006). 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.

2. *Legislative Rule-Selection*

The remaining three 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*

“Reactive” statutes involve legislative authorization of (or limits upon) surveillance practices in the wake of a prior judicial ruling on the constitutional contours of government power. The legislature responds to the prior constitutional decision by defining the circumstances in which the practice is permissible, and the executive follows the legislatively proscribed procedures. The surveillance target, however, might claim that the procedures the legislature authorized are insufficient to meet Fourth Amendment requirements.

Reactive statutes in fact 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. 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”), the legislature may seek to provide more procedural protections than a court has deemed the Fourth Amendment to require.

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. The Wiretap Act responded not only to *Katz*, but also to *Berger v. New York*,³¹ a case from the prior Supreme Court term invalidating a New York statute authorizing surveillance on terms the Court deemed insufficient for Fourth Amendment purposes. In setting the requirements for investigators to follow to obtain a Title III order authorizing electronic surveillance, Congress essentially tracked the Court’s constitutional analysis in *Berger*.³²

³¹ 388 U.S. 41 (1967).

³² The statute at issue in *Berger* allowed court authorization of eavesdropping activities, but the Court found the statutory procedures deficient in several respects. First, the statute required a showing of reasonable grounds to believe that the surveillance would reveal evidence of criminal activity. Although the Court declined to consider whether the “reasonable grounds” standard was equivalent to the Fourth Amendment’s probable cause standard, 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. *Id.* at 55-56. 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. *Id.* at 59-60. Third, the statute allowed law enforcement officials to secure renewal of a surveillance order on the basis of the initial showing. *Id.* at 59. Fourth, the statute did not provide for prior notice of the search to the subject of the surveillance and required no showing of exigency to justify the lack of notice. *Id.* at 60. 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.” *Id.*

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. 18 U.S.C. § 2518(1) (2000). 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. *Id.* § 2518(3). 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. 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. *Id.* § 2518(5). 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. *Id.* §§ 2518(3)(c), 2518(8)(d). 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. *Id.* § 2518(8)(a). The statute also authorizes a judge to require periodic reports on the progress of the surveillance. *Id.* § 2518(6).

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 violated the Fourth Amendment.³³ In holding in *Keith*, however, that 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 surveillance³⁴ and that Congress could properly place the power to review surveillance applications in a specially designated court.³⁵ 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 agent of a foreign power.³⁶ More specifically, it established a specialized court, the FISC, to hear applications for electronic surveillance within the United States to gather foreign intelligence information.³⁷ In light of the *Keith* court’s

³³ 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 (3rd 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).

³⁴ *Keith*, 407 U.S. at 322-23 (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”).

³⁵ *Id.* at 323.

³⁶ *See* 50 U.S.C. §§ 1801-1811 (2000).

³⁷ *See* 50 U.S.C. §§ 1803(a), 1804(a)(7)(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* Patricia L. Bellia, *The “Lone Wolf” Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 430 n.33 (2005). 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. *Id.* §§ 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*, at 441.

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.³⁸

Several statutes fall within the second 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. A portion of the Electronic Communications Privacy Act of 1986³⁹ supplies one example. As a whole, ECPA was designed to update surveillance law to accommodate the development of electronic communications.⁴⁰ The third title of ECPA, however, responded more directly to the Supreme Court's decision in *Smith v. Maryland*, which held that using a “pen register” to acquire the number of an outgoing telephone call is not a search for Fourth Amendment purposes and therefore does not require a warrant.⁴¹ The court's holding would have permitted federal and state officials (absent statutory constraints) to use pen

³⁸ More recently, portions of the USA Patriot Act Improvement and Reauthorization Act, Pub. L. No. 109-177 120 Stat. 193 (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 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 § 115, 120 Stat. at 211, and provided statutory authorization for an NSL recipient to challenge the scope of the NSL in court, *id.* § 116, 120 Stat. at 213.

³⁹ Pub. L. No. 99-508, 100 Stat. 1848.

⁴⁰ See *infra* notes 45-55 and accompanying text.

⁴¹ 442 U.S. 735 (1979).

registers and similar devices without prior judicial authorization. The ECPA provisions thus imposed procedural requirements on the use of pen registers as well as “trap and trace devices” (i.e., devices to detect the number of an incoming call),⁴² requiring that officials seeking to use pen registers or trap and trace devices to certify to a judge that the information in question is relevant to an ongoing investigation.⁴³ The pen register and trap and trace 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.⁴⁴

Although I distinguish here between statutes that implement judicial decisions acknowledging a high level of protection against executive use of a surveillance tactic and statutes that react to judicial decisions denying such protections, it will become clear that *courts’* treatment of the two subcategories or reactive statutes does not differ significantly.

b. *Proactive statutes*

In many cases, the legislature does not await a judicial decision regarding whether a particular executive tactic is constitutional; instead, it selects a rule itself. Within this broad category of “proactive” statutes, it is helpful to distinguish further between two types: “modernizing” statutes—statutes designed to update surveillance law in light of technological developments—and “crisis response” statutes—statutes that respond to a

⁴² ECPA §§ 301-302, 100 Stat. at 1868-72 (codified as amended at 18 U.S.C. §§ 3121-3127 (2000)).

⁴³ 18 U.S.C. § 3121 (2000).

⁴⁴ Other examples, less directly relevant to a discussion of communications surveillance tactics, include the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (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 (responding to the Court’s decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978)). See Peter P. Swire, *Katz is Dead. Long Live Katz.*, 102 MICH. L. REV. 904, 916-17 (2004); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753-60 (2005).

perceived investigative or intelligence failure by authorizing particular surveillance techniques thought lacking in existing law.

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

As noted earlier, The Electronic Communications Privacy Act of 1986 was designed to bring surveillance law authorities into line with technological developments.⁴⁵ 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.⁴⁶ The second segment of the statute established independent protections for stored wire and electronic communications.⁴⁷ These protections, often referred to as the Stored Communications Act (“SCA”), outlawed unauthorized access to a service provider’s facilities to obtain the contents of a wire or electronic communication.⁴⁸ In addition, the SCA prescribed procedures for law enforcement officials to follow to compel production of stored electronic communications from

⁴⁵ See, e.g., 131 Cong. Rec. 24364 (statement of Sen. Leahy); id. at 24396 (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 Favoring Reversal, *United States v. Councilman*, No. 03-1383 (1st Cir. filed Nov. 12, 2004).

⁴⁶ ECPA §§ 101-111, 100 Stat. at 1848-59.

⁴⁷ ECPA §§ 201-203, 100 Stat. at 1860-68 (codified as amended at 18 U.S.C.A. §§ 2701-2709, 2711-2712 (West 2000 & Supp. 2007)).

⁴⁸ 18 U.S.C. § 2701(a) (2000).

service providers;⁴⁹ a subsequent amendment applied these provisions to stored wire communications as well.⁵⁰

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.⁵¹ The amendments to the Wiretap Act put electronic communications on nearly the same footing as wire and oral communications.⁵² Similarly, the purpose of the SCA was to make stored communications less vulnerable to unauthorized acquisition, while preserving law enforcement access to such communications.⁵³

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

⁴⁹ 18 U.S.C. § 2703 (2000).

⁵⁰ USA Patriot Act § 209(1), 115 Stat. at 283.

⁵¹ *See, e.g.*, S. REP. NO. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559, H.R. Rep. No. 99-647, at 19.

⁵² As a concession to the Justice Department, *see* S. Rep. No. 99-541, at 23, *reprinted in* 1986 U.S.C.C.A.N. at 3577, the amendments did not apply all features of the Wiretap Act to electronic communications, but they came close. 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 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.

⁵³ The legislative reports accompanying ECPA acknowledged the legal uncertainty surrounding whether and how the Fourth Amendment might protect such communications. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1413 (2004) (discussing conflicting views of whether subscribers retain an expectation of privacy in communications in the hands of a third party).

would otherwise thwart surveillance.⁵⁴ Eight years later, Congress dealt more directly with the perceived problem of technical developments eroding surveillance capabilities. The Communications Assistance for Law Enforcement Act of 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.⁵⁵

Portions of the USA Patriot Act perhaps provide a final example of a modernizing statute. Although Congress clearly sought in the statute to respond to some perceived gaps in surveillance law in the wake of the September 11 attacks, some portions of the statute had been discussed and proposed for years prior to those attacks.⁵⁶ For example, the USA Patriot Act extended the pen register and trap and trace statute to cover addressing and signaling information associated with electronic communications.⁵⁷ Government agents had previously sought to acquire signaling information associated with electronic communications by invoking the pen register and trap and trace device statute,⁵⁸ despite language ostensibly limiting that statute's reach to wire communications.⁵⁹ Although no court had yet rejected the government's interpretation,

⁵⁴ ECPA § 106(d)(3), 100 Stat. at 1857 (codified as amended at 18 U.S.C. § 2518(11)).

⁵⁵ Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. § 1002(a)(1)-(2) (2000)). 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); Susan Freiwald, *Uncertain Privacy: Communications Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996).

⁵⁶ Consultation and Discussion Draft Bill To Combat Terrorism and Defend the Nation Against Terrorist Acts, and for Other Purposes (Sept. 19, 2001).

⁵⁷ USA Patriot Act § 216, 115 Stat. at 288.

⁵⁸ 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).

⁵⁹ More specifically, the original statute defined a pen register as a device that "records or decodes electronic or other impulses which identify the *number dialed* or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3) (2000) (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).

the Justice Department included a codification of this interpretation in a package of measures proposed in response to the September 11 attacks.⁶⁰

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.⁶¹ In addition to extending the foreign power definition well beyond that appearing in the original statute, Congress has since added three new titles to FISA, one allowing the FISC to approve physical searches,⁶² one allowing the FISC to approve the use of pen registers and trap and trace devices,⁶³ and one allowing the FISC to approve the compelled production of certain records.⁶⁴ Each title responded to particular intelligence failures that the executive identified or Congress perceived (or concerns that government tactics undertaken without judicial authorization would subsequently be rejected in court).⁶⁵ For this article’s focus on communications

⁶⁰ [ADD CITE]

⁶¹ Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

⁶² 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. §§ 1821-1829 (2000 & Supp. IV 2004)).

⁶³ Intelligence Authorization Act for Fiscal Year 1999, § 601, 112 Stat. at 2405 (codified as amended at 50 U.S.C.A. §§ 1841-1846 (West 2000 & Supp. 2007)).

⁶⁴ 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)). 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 (codified as amended at 50 U.S.C.A. §§ 1861-1862 (West 2000 & Supp. 2007)) (deleting former §§ 1861-1863 and adding new §§ 1861-1862 authorizing orders to compel production of tangible things).

⁶⁵ 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 arose indirectly from the 1995 Oklahoma City bombing. Investigators who initially believed the bombing was the work of foreign terrorists had been unable to secure certain records

surveillance tactics, the most relevant of these new 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.⁶⁶ The amendment thus created on the foreign intelligence side a pattern similar to that on the criminal side, with investigators having the ability to request an order permitting the use of a pen register or trap and trace device on a lower predicate than is required for other forms of electronic surveillance.⁶⁷

Portions of the USA Patriot Act also serve as obvious examples of the crisis response model. Among the Act's provisions are several designed to respond to specific perceived intelligence failures in connection with the September 11 attacks. Perhaps the most controversial of these was the dismantling of the "wall" that separated criminal investigators and counterintelligence investigators within the Justice Department and the Federal Bureau of Investigation in investigations involving FISA.⁶⁸ The USA Patriot Act similarly loosened restrictions in the Wiretap Act on the sharing of information among

concerning the rental truck seen near the site of the bombings. [CITE; *cf.* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1329 (1994).] 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 also* USA Patriot Act § 215 (codified as amended at 50 U.S.C.A. §§ 1861-1862 (West 2000 & Supp. 2007)) (deleting former §§ 1861-1863 and adding new §§ 1861-1862 authorizing orders to compel production of tangible things).

⁶⁶ [DOJ source; need confirmation.]

⁶⁷ Other amendments to FISA 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, §§ 601-602, 114 Stat. 2831, 2850 (2000). These changes responded to a perceived failure in the handling of the Wen Ho Lee matter. *See* S. REP. NO. 106-352 (2000).

⁶⁸ *See* Bellia, *supra* note 37, at 452-56.

agencies. Before September 11, the Justice Department had interpreted a Wiretap Act provision authorizing law enforcement officials to share intercepted communications with “another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure” to limit sharing with intelligence officials.⁶⁹ The USA Patriot Act added language specifically allowing disclosure of the fruits of Title III surveillance to intelligence officials and others.⁷⁰

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.⁷¹ 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 search 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.⁷² Adopted in 2004 as part of a broader intelligence bill, the lone wolf

⁶⁹ 18 U.S.C. § 2517(1). Law enforcement officials could share such information to receive specific information relevant to the investigation, but could not on a wholesale basis turn the fruits of electronic surveillance over to intelligence agencies. [OLC Opinion]; *see also* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1181 & n.236 (2004).

⁷⁰ USA Patriot Act § 203(b), 115 Stat. at 280 (codified at 18 U.S.C.A. § 2517 (West 2007)) (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).

⁷¹ *See* 50 U.S.C. § 1801(a)(4), (b)(1)(A), (b)(2)(C) (2000).

⁷² *See* Bellia, *supra* note 37, 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 (Norton 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

amendment expanded FISA’s 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.⁷³ 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.⁷⁴

B. *Understanding the Judicial Landscape*

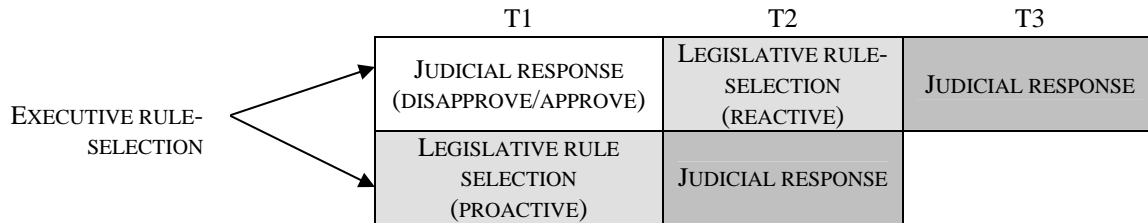
Analyzing judicial outcomes through the lens of the institutional patterns outlined above permits a more nuanced view of executive, legislative, and judicial involvement in the formulation of communications surveillance law. The graphic below reflects several of the postures in which a court will be called upon to assess the executive’s use of a particular surveillance law technique. The graphic presumes that the executive chooses in the first instance which procedures to follow before engaging in a particular surveillance activity. Sometimes judicial review will follow the executive’s action (at T1), the legislature (at T2) will react to the judicial decision, and a further challenge to the legislature’s selection of a rule will follow (at T3). In other cases, the legislature will respond proactively to the executive’s action (at T1) before a court has acted, and judicial

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. The 9/11 Commission Report identifies Moussaoui as a potential substitute pilot for United Airlines Flight 93.

⁷³ 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 therefor.” Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (codified at 50 U.S.C. § 1801(b)(1)(C)).

⁷⁴ *See, e.g., Amendments to the Foreign Intelligence Surveillance Act: Hearings on S. 2586 and S. 2659 Before the Senate Select Committee on Intelligence*, 107th Cong. 14-19, 20-21 (2003) (statement and testimony of Marion E. “Spike” Bowman, Deputy General Counsel, FBI).

review will only follow (at T2) once the legislature has chosen what it perceives to be the best approach.



These patterns of decision-making prove important in evaluating descriptive claims about the role of courts in regulating communications surveillance tactics. Judicial evaluation of the constitutionality of a surveillance tactic can arise at T1 in response to executive rule-selection, at T3 in response to legislative rule-selection in reaction to a prior judicial decision, or at T2 in response to a proactive legislative rule (such as a modernizing or crisis-response statute). It would not be surprising to find, for example, that courts do more intervention at T1 and less at T3. If we unpack claims about judicial “deference” to legislative judgment regarding surveillance tactics, however, we find that they generalize about judicial responses at quite different phases.

Consider in particular Professor Kerr’s historical claim that courts frequently defer to Congress’s decisions about what level of privacy to afford emerging technologies—a claim that provides important support to his normative claim that courts *should* defer to legislative decisions about how to regulate new surveillance technologies. Among the trends that Professor Kerr cites as confirming historical legislative supremacy in surveillance law⁷⁵ are that: (1) Congressional action followed soon after the *Berger*,

⁷⁵ 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

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 challenges⁷⁶ and challenges to specific statutory gaps (such as the exclusion of cordless phones from the statute until 1994⁷⁷); 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. We could characterize each of these developments quite differently.

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 at T1 above—it faces a different question of deference than it does at T2 or T3 in response to legislative rule-selection. Neither a court nor a legislature has assessed the privacy implications of the practice. For this reason, it is not surprising to find some significant judicial activity in this category. *Berger*, *Katz*, and *Keith* provide examples of such activity, as does the recent district court decision declaring the NSA terrorist surveillance program unconstitutional.⁷⁸ Legislative action of course followed the *Berger*, *Katz*, and *Keith* decisions, and case-by-case adjudication of surveillance

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 19, 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.

⁷⁶ See Kerr, *supra* note 19, at 850 (“The judiciary’s deferential stance began with the case law that followed the passage of Title III.”)

⁷⁷ *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.”).

⁷⁸ *Am. Civil Liberties Union v. Nat’l Security Agency*, 438 F. Supp. 2d 734 (E.D. Mich. 2006).

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.⁷⁹ Congress placed video surveillance outside of the ambit of the Wiretap Act, but courts imposed the Wiretap Act's requirements anyway. To be sure, as Professor Kerr points out, courts adopted the Wiretap Act's requirements rather than "creat[ing] new judicial standards from scratch."⁸⁰ Adoption of those requirements, however, was premised upon a threshold determination that Professor Kerr implicitly expects, if not explicitly urges, courts to leave to the legislature: that the technique invades a reasonable expectation of privacy. It is therefore difficult to characterize those decisions as involving judicial deference to legislative choices.

Of course, courts do not always respond to executive rule-selection by demanding stringent procedures. For example, many scholars have been highly critical of the Supreme Court's determination in *Smith v. Maryland* that the Fourth Amendment permits warrantless use of pen registers and similar devices. 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 dispute⁸¹ than in what it tells us about the relative roles of courts and legislatures.

⁷⁹ See *supra* note 13 (citing cases).

⁸⁰ Kerr, *supra* note 19, at 854.

⁸¹ I have discussed the shaky doctrinal underpinnings of *Smith v. Maryland* elsewhere. See Bellia, *supra* note 53, at 1397-1413.

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 does not make the primary architect of the surveillance law scheme, particularly when the procedural provisions barely exceed the constitutional minimum.

2. *Legislative Rule-Selection*

a. *Reactive statutes*

Moving to *reactive* statutes, the absence of successful constitutional challenges in this context (at T3) is unsurprising. Where a court has disapproved of a particular executive tactic (at T1) and the legislature responds (at T2) by implementing the judicial decision, further judicial intervention (at T3) 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.⁸² The failure of facial challenges thus 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

⁸² See Kerr, *supra* note 19, at 851; see also Bellia, *supra* note 53, at 1388-91 (describing protections).

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 will not invalidate a reactive legislative rule that seeks to enhance those safeguards. In short, very little can be gleaned from the absence of successful constitutional challenges among reactive statutes.

b. *Proactive Statutes*

Proactive statutes raise more difficult questions. Although Congress, rather than the executive, takes the first cut at developing a Fourth Amendment–compliant framework, it does not do so against the backdrop of a prior judicial determination whether use of the tactic invades a reasonable expectation of privacy. As a result, the absence of successful Fourth Amendment challenges in this context cannot necessarily be explained as a situation of courts and the political branches simply relying on the same clearly authoritative sources of law to assess the issue. No well-developed law exists.

Modernizing statutes. Specifically with respect to modernizing statutes, one could explain the absence of judicial review in this context as Professor Kerr does—as reflecting a decision to defer to Congress’s superior judgment on fast-moving technology. That is one plausible explanation, although the absence of judicial review in this context does not permit us to rule out an alternative explanation: that a court would be unlikely to dislodge even a highly questionable factual judgment about the path of technology.

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 two problems with such an inquiry in this context. First, as currently understood, the reasonable expectation of privacy test takes account of society's perceptions of the vulnerability of communications to unauthorized acquisition. Engaging in such an inquiry with respect to an emerging communications medium requires a heavily empirical analysis by a court to assess what society's perceptions are.⁸³ Second, 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 medium to be vulnerable.

As time goes on, moreover, it may become increasingly difficult for a court to dislodge erroneous congressional judgment 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 to regulate that technology. Assume also that courts initially rejected 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

⁸³ Susan Freiwald, *First Principles of Communications Privacy* (unpublished manuscript, on file with author); cf. [Kerr unpublished manuscript].

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. It is equally plausible, however, that the statute reflects ossified and inadequately protective rules, but is difficult to dislodge in light of the nature of the reasonable expectation of privacy inquiry and a reluctance to disturb a statutes on the books for many years. Perhaps the Stored Communications Act comes closest to illustrating these difficulties. As noted, until the *Warshak* decision, no court had questioned the constitutionality of the SCA’s government access provisions. Yet the government has long interpreted those provisions to allow its agents to compel production of broad categories of stored electronic communications (and, after passage of the USA Patriot Act, stored wire communications as well) without demonstrating probable cause to a judge.

The government’s position is based on a statutory distinction between communications “in electronic storage” and those that are not, and between providers of “electronic communication services” and providers of “remote computing services.” In particular, communications in electronic storage with the provider of an electronic communication service for 180 days or less receive warrant-like protection;⁸⁴ communications not in electronic storage, maintained for longer than 180 days, or maintained with a remote computing service do not.⁸⁵ The government interprets the term “electronic storage” narrowly, to encompass only temporary storage on a provider’s

⁸⁴ 18 U.S.C. § 2703(a).

⁸⁵ 18 U.S.C. § 2703(b).

server before the user retrieves the message.⁸⁶ Once a user retrieves the message, any copy that the user leaves on the provider's system is, under the government's theory, held by a remote computing service and subject to the lower government access standards.⁸⁷ The literal definition of the term "remote computing service" covers providers that offer "storage" services to the public.⁸⁸ The government thus treats e-mail already accessed by a subscriber but left on the provider's system as e-mail stored by a remote computing service "on behalf of, and received by means of electronic transmission from . . . a subscriber or customer."⁸⁹ The SCA permits agents to compel production of communications from a remote computing service through a number of avenues: by presenting a warrant, by obtaining an order from a court after demonstrating specific and articulable facts that the material sought was relevant to an ongoing criminal investigation, or by issuing an administrative or grand jury subpoena.⁹⁰

At the time of ECPA's adoption, the narrow coverage of the term "electronic storage" was perhaps unproblematic. In 1986, electronic communications were of course not widely used for personal purposes.⁹¹ In addition, long-term storage of electronic communications with a provider that facilitated transmission of those communications was too expensive to be routine.⁹² At the time of ECPA's adoption, the lower standard

⁸⁶ That interpretation is based on section 2510(17)'s definition of "electronic storage" as encompassing "temporary, intermediate storage incidental to the transmission of a communication. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 88-89 (2002), <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm> [hereinafter CCIPS MANUAL].

⁸⁷ *Id.*

⁸⁸ 18 U.S.C. § 2711(2) (2000).

⁸⁹ 18 U.S.C. § 2703(b)(2)(A) (2000).

⁹⁰ 18 U.S.C. § 2703(b) (2000 & Supp. IV 2004); 18 U.S.C. § 2703(d) (2000).

⁹¹ 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).

⁹² *Id.* at 1569.

for communications held by a provider of remote computing services was probably also unproblematic. The “remote computing service” term can be more readily understood in the context of the computing industry at the time of the statute’s passage. Because computing capacity and storage was still relatively expensive, a business might outsource certain processing and data storage tasks; the statute treated a company that performs such storage and processing services as the provider of a “remote computing service.”⁹³ 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 items in which one could have a reasonable expectation of privacy.⁹⁴ In short, the SCA contemplated both short-term storage of electronic storage of communications with a communications provider and longer-term storage of records with a remote computing service provider. The SCA did not clearly contemplate long-term storage of personal communications with a communications provider.

Even if these distinctions were plausible in 1986, the technological environment within which the distinctions now apply has changed dramatically. In 1986, it was likely that users would have had to take affirmative steps to retain e-mail messages they already accessed.⁹⁵ 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 is correct, however, all opened messages that remain on systems like Gmail are not subject to the higher warrant-like protections of section 2703(a) of the SCA.

⁹³ U.S.C. § 2711(2) (2000).

⁹⁴ See *United States v. Miller*, 425 U.S. 435 (1976); see also Bellia, *supra* note 53, at 1397-1413 (discussing *Miller*); Mulligan, *supra* note 91, at 1569.

⁹⁵ Mulligan, *supra* note 91, at 1569.

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. In defending the constitutionality of the statute in *Warshak*, however, the government has quite naturally pointed out that, in twenty years, no court has ever declared these provisions of the SCA unconstitutional.⁹⁶

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. The absence of judicial intervention may indeed signal Congress’s superiority in setting flexible and adequately protective rules for developing technologies. But we cannot rule out the possibility that the shifting technological landscape has destabilized the structure of a statute that was once plausibly viewed as constitutional.

Crisis response statutes. In the other category of proactive statutes—those involving Congress’s response to a perceived gap in surveillance law—courts have also taken a hands-off approach. Again, as Professor Kerr suggests, that approach may reflect deference to Congress’s superior ability to weigh privacy interests in relation to particular law enforcement and intelligence needs. As with modernizing statutes, however, we cannot rule out the alternative explanation that Congress underprotects privacy in this context and courts are ill-equipped to respond.

⁹⁶ Brief for Defendant-Appellant United States at 14, *Warshak v. United States*, No. 06-4092 (6th Cir. filed Oct. 11, 2006) (“For twenty years, the Stored Communications Act has set for the procedures for the government to follow to compel disclosure of e-mail, and no court has previously found it to be unconstitutional.”).

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, insofar as *Keith* explicitly contemplates that national security investigations may present “different policy and practical considerations from the surveillance of ‘ordinary crime’”⁹⁷ and yield 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.”⁹⁸ This test remains underdeveloped in the law, and as a result operates as a fairly soft limit on congressional action.⁹⁹

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*,¹⁰⁰ had held that warrantless surveillance was unlawful once the gathering of foreign intelligence was no

⁹⁷ *Keith*, 407 U.S. at 322.

⁹⁸ *Id.* at 322-23.

⁹⁹ Bellia, *supra* note 37, at 449-52.

¹⁰⁰ 456 F. Supp. 51 (E.D. Va. 1978).

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.¹⁰¹ Although FISA as enacted simply required certification as to “the” purpose of the surveillance, defendants challenging FISA surveillance drew upon the *Humphrey* case to 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.¹⁰²

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.¹⁰³ These guidelines were prompted in part by concern that a court following the *Humphrey* court’s logic would use contacts between counterintelligence and criminal investigators as the measure of the purpose of FISA surveillance. 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 to orders approving surveillance requests.

When the Justice Department sought modification of the guidelines the FISC imposed, the FISC rejected its request. Not only did the FISC not decide the case on

¹⁰¹ *Id.* at 59.

¹⁰² Bellia, *supra* note 37, at 454.

¹⁰³ 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>.

constitutional grounds, it claimed that the case raised no constitutional issue¹⁰⁴—even though the evolution of the 1995 guidelines could be traced back to a Fourth Amendment decision. The underdevelopment of the law in this area, however—a function of the FISC’s secrecy and the infrequency with which FISA issues arise in other courts—makes a constitutional ruling against the amendment unlikely. In reversing the FISC’s statutory holding and concluding that the proposed Justice Department guidelines did not violate the Fourth Amendment, the Foreign Intelligence Surveillance Court of Review observed that the constitutional question “has no definitive jurisprudential answer,” for it turns on the reasonableness of the procedures in relation to the differences outlined in *Keith* and subsequent cases between national security surveillance and surveillance related to ordinary crime: differences with respect to 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).¹⁰⁵

A court considering a Fourth Amendment challenge to a crisis response statute in the immediate aftermath of its enactment will not lightly disregard Congress’s assessment of the importance of the government’s interest. Again, the point here is not that the FISC’s decision is correct or incorrect. The point, rather, is that a norm of judicial deference to Congress’s superior ability to weigh privacy and law enforcement interests is not necessarily at work here. The outcome is equally consistent with a quite different

¹⁰⁴ See *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 614 (For. Intell. Surv. 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.”).

¹⁰⁵ See Bellia, *supra* note 37, at 450-51 (culling these factors from *Keith* and subsequent decisions rejecting Fourth Amendment challenges to FISA).

narrative—one of legislative and judicial underprotection of privacy interests in the face of urgent investigative demands.

3. *Summary*

Several key points emerge from this discussion. First, simply 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, a great deal of 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. It is true that where the legislature moves proactively, and acts when a court has not spoken with respect to the tactic in question, courts have played a less visible role. Whether that state of affairs reflects a welcome norm of judicial deference to legislative action, or the problems of dislodging erroneous decisions about the path of technology (in the case of modernizing statutes) and isolating the influence of perceptions about the importance of government interests (in the case of crisis response statutes), remains to be seen.

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, first, that both the judicial abdication perspective and the legislative supremacy perspective understate the role of courts. But although much of the judicial silence on the constitutionality of surveillance law tactics is attributable to the

particular posture in which a constitutional claim arises, cases involving “proactive” surveillance law regulations cannot be so easily explained; the outcomes are consistent either with a legislative supremacy narrative or a judicial abdication narrative.

The irreconcilability of these narratives leads us to more functional questions about how courts *should* behave—that is, about the relative competence of legislatures and courts to provide appropriate checks on executive conduct in this area. Analyzing the institutional competence arguments, particularly in light of the surveillance law patterns identified above, reveals that current accounts tend to ignore both the sequential nature of decision-making in surveillance law, and, relatedly, how design choices affect the quality of decisions.

This Part fleshes out this claim and seeks to draw “second-order” design questions into the debate. Section A begins by exploring institutional competence arguments through the lens of the institutional patterns identified above. Section B disentangles the relationship between “second-order” design questions and 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, in addition to offering divergent accounts of why courts have not engaged in much constitutionally-based surveillance law regulation since *Katz*, scholars offer different views on what role courts *should* play. These views implicitly or explicitly reflect arguments about institutional competence. Judicial abdication scholars, for example, see Congress as having been largely “captured” by law enforcement

interests on these issues.¹⁰⁶ Legislative supremacy scholars, in contrast, focus on how Congress can respond quickly to rapid technological changes, whereas courts can only make incremental decisions about the path of technology, and then only in the context of a concrete case perhaps presenting an outdated record.¹⁰⁷

Institutional choice methodologies are of course controversial in many respects.¹⁰⁸ Because functional arguments play an important role in debates over how courts and Congress should regulate surveillance technologies, however, I simply seek to take that debate on its own terms. 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;¹⁰⁹ 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. Although these issues are important, here I focus on a broader problem with institutional competence arguments in this context: their failure to account for how design choices affect the quality of judicial and legislative decisions, particularly in the case of iterative or sequential decision-making.

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 identify the

¹⁰⁶ See, e.g., Swire, *supra* note 44, at 914 (likening law enforcement agencies to regulated industry); Swire, *supra* note 65, at 1348-50 (describing public choice realities of how surveillance legislation is enacted).

¹⁰⁷ Kerr, *supra* note 19, at 864-82.

¹⁰⁸ Cf. Solove, *supra* note 44, at 760; [ADD CITES].

¹⁰⁹ See, e.g., Swire, *supra* note 44, at 914.

institution that is best positioned to do so, identifying the overarching social 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 “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.¹¹⁰ The social 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.

¹¹⁰ Freiwald, *supra* note 17, at 19-20.

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. Indeed, in arguing that functional considerations should lead courts to be “cautious” in evaluating challenging the use of new search technologies, Professor Kerr does not confine his claim to situations where Congress has already passed a (proactive or reactive) statute regulating the practice. As a result, 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 competencies (as legislative supremacy scholars do) is not enough to justify the approach.

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, the binary legislature versus courts approach to regulating surveillance tactics ignores how institutional decisions proceed in sequence and constrain later institutional options. Suppose we choose the legislature as the preferred institution to

rein in executive tactics, based on conclusions about judicial competence. The legislature sets restrictions on executive conduct. It is likely, however, that some interpretive decisions will fall to courts. When faced with those interpretive decisions, courts must choose whether to narrowly or broadly construe statutory provisions. How should institutional competence concerns enter into this picture, if at all? The same doubts about judicial competence might counsel in favor of a court staying its hand, and narrowly construing the statute. As in an executive rule selection case, however, a narrow construction essentially privileges the *executive's* position on the scope of its power. In short, the legislative supremacy position essentially requires different functional arguments to justify narrowly applying the Fourth Amendment but broadly construing statutes,¹¹¹ when in reality the arguments likely point in the same direction.

Indeed, one could argue that statutory surveillance law questions are harder to resolve than constitutional ones, or at a minimum that statutory interpretation questions are more easily resolved with constitutional considerations in the background.

Construction of provisions at the intersection of the Wiretap Act and the Stored Communications Act provide one example.

In *United States v. Councilman*, a district court considered whether an Internet service provider that captured communications of its customers before transmitting them into users' mailboxes had "intercepted" those communications. The communications were acquired during a brief period of storage in the ISP's system before transmission to

¹¹¹ Professor Kerr, for example, himself suggests the possibility of "judicial caution in the statutory area and judicial boldness in the statutory area" as an "optimal solution." Orin S. Kerr, *Technology, Privacy, and The Courts: A Reply to Colb and Swire*, 102 MICH. L. REV. 933, 940 (2004); see also Solove, *supra* note 44, at 767 ("In reality, Kerr's argument concerns only whether Fourth Amendment rules interpreted by judges are preferable to statutory rules interpreted by judges. In fact, judges have frequently botched interpreting statutory law, as Kerr repeatedly has lamented.").

the user's mailbox.¹¹² Because the communications were acquired during this brief period of storage, the district court had concluded that the communications were not intercepted for purposes of the Wiretap Act,¹¹³ and the Court of Appeals for the First Circuit affirmed on the same reasoning.¹¹⁴

The courts' conclusion that a service provider can acquire the contents of a communication prior to completion of the transmission phase, merely because it is stored at a point in the transmission process, had profound implications for government access to electronic communications, because the government may 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.¹¹⁵ Had the courts fully considered the constitutional implications of that fact, particularly in light of the *Berger* Court's analysis, it seems unlikely that they would have reached the same result. The constitutional avoidance issue was briefed before the *en banc* First Circuit,¹¹⁶ which ultimately reversed the district court.¹¹⁷

Second, apart from the problem that competency arguments largely cut across constitutional and statutory questions, 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

¹¹² *United States v. Councilman (Councilman II)*, 373 F.3d 197, 199 (1st Cir.), 373 F.3d 197 (1st Cir.), *pet'n for reh'g en banc granted*, 385 F.3d 793 (1st Cir. 2004), *rev'd*, 418 F.3d 67 (1st Cir. 2005).

¹¹³ *Councilman I*, 245 F. Supp. 2d 319, 321 (D. Mass. 2003).

¹¹⁴ *Councilman II*, 373 F.3d at 204.

¹¹⁵ *See, e.g.*, Brief on Rehearing *En Banc* for Senator Patrick J. Leahy as *Amicus Curiae* Supporting the United States and Urging Reversal, *United States v. Councilman* 10-11 (1st Cir. filed Nov. 12, 2004) (No. 03-1383), *available at* <http://www.cdt.org/wiretap/20041112leahy.pdf>; Supplemental Brief of Center for Democracy and Technology et al., *United States v. Councilman* 1-4 (1st Cir. filed Nov. 12, 2004) (No. 03-1383), *available at* <http://www.cdt.org/wiretap/20041112joint.pdf>.

¹¹⁶ Supplemental Brief of Center for Democracy and Technology et al., *United States v. Councilman* 1-4 (1st Cir. filed Nov. 12, 2004) (No. 03-1383), *available at* <http://www.cdt.org/wiretap/20041112joint.pdf>.

¹¹⁷ 418 F.3d at 67.

or the SCA. The lack of a suppression remedy limits courts' ability to address questions of statutory interpretation—perhaps perpetuating impressions of judicial inability to 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 likely 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, it is worth making two additional points with respect to proactive statutes. First, I noted that Congress often confides important statutory questions to courts, but in the particular context of ECPA has limited courts' ability to interpret the relevant provisions by withholding a statutory suppression remedy. No doubt that omission was motivated in part by a belief that no suppression remedy was warranted,¹¹⁸ 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 not only hamper 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 (as Professor Kerr notes), Congress updated ECPA on 11 occasions between its passage in 1986 and the year 2002, most of the amendments

¹¹⁸ See *supra* note 52 (noting that Justice Department demanded omission of suppression remedy).

preceding the Patriot Act reflected 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 the appropriate response to modernizing and crisis response statutes.¹¹⁹ Rather, it is to suggest that institutional competence arguments tend to overgeneralize in light of the nature and realities of surveillance regulation. First, because of the iterative nature of surveillance law regulation, a binary legislature versus courts approach misses the manner in which one institution's decisions constrain or eliminate the possibility of another's response. Second, such analyses take institutional design features as a given, thus overlooking the possibility that changes in institutional design could be used to *improve* the quality of legislative and judicial decisions.

B. *Second-Order Design Questions*

As the previous section illustrated, one of the difficulties with evaluating institutional competence arguments about surveillance law is that such analyses tend to take institutional design as a given. That approach does not take account of how institutions respond to one another in ways that affect the quality of decisions that an institutional competence model will predict. 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.

¹¹⁹ 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).

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 (information concerning a crime that has been, is being, or will be committed), how much (renewable periods of up to 30 days), and for what purpose (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 Wiretap Act's structure, which allocates implementation of restrictions on what kind of information agents can seek to a combination of executive and judicial authorities. 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.¹²⁰ In theory, the effect of such a requirement is to centralize decision-making and vest it in politically accountable officials, and perhaps even place certain executive officials in a quasi-judicial role. By

¹²⁰ 18 U.S.C. § 2516(1), (2) (2000 & Supp. IV 2004).

most accounts, in practice this requirement has had the effect of making the wiretap application process a fairly burdensome one for investigators.¹²¹ The Wiretap Act’s high-level executive review requirements have 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).¹²² Other aspects reflect a different allocation. Law enforcement officials must “minimize” interception of communications not authorized to be intercepted, but judicial checks on whether they have done so are limited.¹²³ 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.¹²⁴ The statute does, however, require judicial evaluation of whether other-crimes evidence should be admitted into court.¹²⁵

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, different design combinations are available to meet first-order preferences. A goal of preventing unlawful executive surveillance, for example, might be equally achieved through a statutory

¹²¹ 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 38, at 470.

¹²² 18 U.S.C. § 2518(3); *id.* § 2510(9)(a).

¹²³ 18 U.S.C. § 2518(5).

¹²⁴ 18 U.S.C. § 2517(5).

¹²⁵ *Id.*

suppression mechanism and through the availability of a civil damages remedy against executive officials who authorize the surveillance.

2. *Constitutional Constraints*

It is important to consider 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. Current Fourth Amendment doctrine thus acts as a backstop to normative arguments about executive discretion in surveillance law, for it prevents government from moving to a model involving too much attention to privacy interests. Beyond that, however, the Constitution imposes minimal constraints on first-order preferences, for nothing prevents the choice of a more privacy-oriented balance point when the Fourth Amendment does not require it. Similarly, regarding second-order questions about implementation of first-order preferences for limits on executive surveillance tactics, 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 to assess reasonableness. 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 real-time data concerning the particular cell phone towers “hit” by a cell phone. By acquiring such data from cell phone providers in real time, law enforcement officials can “triangulate” the data and track the location of the of the targeted cell phone.

The authority under which officials can compel a provider to produce such data is very much in dispute. 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 statute¹²⁶ and a portion of the Stored Communications Act governing disclosure of customer records.¹²⁷ That approach was based on the theory that: (1) information concerning a cell phone’s contact with cell towers literally fell within the provision authorizing officials to obtain orders for the use of pen registers and trap and trace devices, because that provision covers devices used to obtain “signaling” information; (2) a separate statute, the Communications Assistance for

¹²⁶ 18 U.S.C. § 3121.

¹²⁷ 18 U.S.C. § 2703(d).

Law Enforcement Act, barred officials from relying solely on the pen register and trap and trace statute to obtain location information; and (3) a “hybrid” order under the pen register and trap and trace provisions and the SCA’s customer records provisions would be sufficient to compel production of that information.¹²⁸

Numerous magistrate judges accepted the government’s argument and granted the requested “hybrid” order. [*Readers: I have omitted from this paragraph a discussion of two cases in which magistrate judges separately invited amici to respond to the government’s ex parte requests for a “hybrid” order. The relevant facts came from discussions with the judges’ chambers and need to be cleared before distribution.*] In converting the proceeding from an *ex parte* proceeding to a quasi-adversarial one, the courts effectively lowered the institutional barriers to participation by potential surveillance targets (as represented by privacy groups).¹²⁹

¹²⁸ See, e.g., *In re Application of the United States*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005).

¹²⁹ The two decisions, which held that the government could not obtain the information without a warrant supported by probable cause, launched a trend among magistrate judges of rejecting the government’s “hybrid” authority theory. See *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F.Supp.2d 947 (E.D. Wis. 2006); *In re Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Information*, 407 F.Supp.2d 134 (D.D.C. 2006); *In re Application of the U.S. for an Order Authorizing Installation and Use of Pen Register*, 415 F.Supp.2d 211 (W.D.N.Y. 2006); *In re Application of United States for an Order Authorizing the Installation and Use of a Pen Register*, 402 F.Supp.2d 597 (D. Md. 2005); *In re Application of the United States for an Order*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005).

Although the above-cited cases all require a warrant based on probable cause when the government seeks to “triangulate” cell phone data to yield a suspect’s physical location, other courts have accepted the “hybrid” order theory when officials seek not real-time data concerning multiple cell towers in range of the suspect’s phone, but rather historical data about the single cell towers carrying the suspect’s call at the beginning and end of the call (which will yield only the target’s general location). See *In re Application of the U.S. for an Order*, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006); *In Matter of Application of U.S. for an Order*, 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005). Other courts have insisted on a warrant even in this situation. See *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 2006 WL 2871743, at *5 (E.D. Wis., Oct. 6, 2006); *In re Application for an Order Authorizing the Installation of Pen Register and Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the Number [Sealed]*, 439 F.Supp.2d 456, 457 (D. Md. 2006); *In re Application of the U.S.*, 441 F.Supp.2d

The insights of comparative institutional analysis theorists help to illustrate how potential shifts in participation costs can affect the opportunities for legal rule changes. In particular, Professor Neil Komesar’s “participation-centered” framework facilitates comparisons of institutional performance by exploring, across institutions, differences among those seeking legal change in terms of the in costs and benefits of institutional participation.¹³⁰ 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.¹³¹

By opening the cell site cases to *amici* participation, the judges in those cases shifted the 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 rule-selection in the

816, 827-28 (S.D. Tex. 2006); In re Application of the U.S., 2006 WL 1876847 (N.D. Ind., July 5, 2006); In re Application of the U.S. for an Order for Prospective Cell Site Location Information, 2006 WL 468300, at *2 (S.D.N.Y. 2006); In re U.S. for Orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices, 416 F.Supp.2d 390, 396 (D. Md. 2006); In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 407 F.Supp.2d 132, 133 (D.D.C. 2005).

¹³⁰ NEIL KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 8 (1994).

¹³¹ *Id.*

first instance. By soliciting *amicus* participation, the cell site 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 discuss categories of 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 article.

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*

Here 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.¹³² In short, whether in legislative or judicial fora,

¹³² [Explain post-Patriot Act dynamics of nationwide jurisdiction provisions.]

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 law enforcement 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.¹³³

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. Those 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.¹³⁴ No statutory suppression remedy is available under the SCA.¹³⁵

¹³³ 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); see also Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1341 (2005) (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).

¹³⁴ 18 U.S.C. § 2515, 2518(10)

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, for 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,¹³⁶ as well as other assistance provisions in surveillance law statutes themselves,¹³⁷ dramatically limit providers' incentives to seek restraints on executive discretion in surveillance law. Indeed, although government officials have reportedly used tens of thousands of national security letters to seek information from various record holders,¹³⁸ and presumably a sizable number of these letters were issued to communications providers under the SCA's NSL provisions, there have been only two publicly reported instances of providers challenging NSLs.¹³⁹

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.

¹³⁵ *Id.* § 2708 (providing that civil remedies are exclusive nonconstitutional remedies for violations of SCA).

¹³⁶ *See* 47 U.S.C. § 1008.

¹³⁷ *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).

¹³⁸ *See* Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A1.

¹³⁹ *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005)

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,¹⁴⁰ a surveillance target only receives notice that of the surveillance when the government intends to introduce FISA-derived information in a judicial or other proceeding.¹⁴¹ Although there have been more than 17,000 FISA applications and renewals granted since 1979, challenges to introduction of FISA-derived evidence have been brought in approximately twenty cases¹⁴² and none of these challenges has been successful.¹⁴³ Because questions concerning the legality of particular searches 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

¹⁴⁰

¹⁴¹ See 50 U.S.C. § 1806(c), (d). 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).

¹⁴² The number in the text reflects cases published in the national reporter system or available on Westlaw or Lexis. It includes fifteen cases in which a defendant in a criminal case moved to suppress FISA-derived evidence (including eleven cases in which a court of appeals affirmed denial of a suppression motion and four cases decided at the district court level and apparently not appealed), as well as five cases adjudicating the legality of a FISA surveillance or search in some other procedural posture (such as 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). 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.

¹⁴³ 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.

particular crisis, such as that in the wake of the Wen Ho Lee investigation.¹⁴⁴ 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 release 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.¹⁴⁵ 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.¹⁴⁶ 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.”¹⁴⁷ The statute also requires the Attorney General to “fully inform” the

¹⁴⁴ See 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> [hereinafter BELLOWS REPORT]; GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 11-15 (2001) [hereinafter GAO COORDINATION REPORT].

¹⁴⁵ Bellia, *supra* note 37.

¹⁴⁶ 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.

¹⁴⁷ 50 U.S.C. § 1807 (2000).

congressional intelligence committees “concerning all electronic surveillance” under FISA.¹⁴⁸ 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 to continue in effect.¹⁴⁹ All of these reports were made public.¹⁵⁰ 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 officials 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 in which interpretations of surveillance law statutes will arise in purely civil disputes to which the government is not a party, when the interpretations will bear upon the scope of agents’ authority. Because courts appear to readily accept *amicus* participation by the United States in such cases, institutional barriers remain low.

¹⁴⁸ *Id.* § 1808(a).

¹⁴⁹ *Id.* § 1808(b).

¹⁵⁰ See S. Rep. 98-660 (1984); H.R. Rep. 98-738 (1984); S. Rep. No. 97-691 (1982); H.R. Rep. 97-974 (1982); S. Rep. No. 97-280(1981); H.R. Rep. 97-318 (1981); S. Rep. No. 96-117 (1980); H.R. Rep. No. 96-1466 (1980); No. 96-379 (1979); H.R. Rep. No. 96-558 (1979).

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; particularly when providers are not forced to bear the cost of surveillance tactics, they have limited incentives to oppose government demands for more surveillance power. In the judicial process, a provider that receives a surveillance order may seek to quash the application. Although there are no institutional barriers to its participation, a service provider's incentives to challenge government surveillance tactics will 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.¹⁵¹

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 obviously 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 involved. In late 2006, for example, the government filed an application in the Southern District of New York seeking disclosure of the contents of instant messages logged with a service provider.

¹⁵¹ See *supra* notes XX-XX.

When the court notified the government that it intended to invite *amicus* participation and request briefing, the government immediately withdrew the application.¹⁵²

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. 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. In the wake of the September 11 attacks, Congress loosened the necessary

¹⁵² [Bankston e-mail]

showing of purpose and dramatically expanded the category of items that could be compelled from third parties to encompass tangible things rather than business records.

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 interests 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.¹⁵³ 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.¹⁵⁴ 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: *ex parte* review of an application for surveillance, review of a communication provider's objection to an order (presumably in the context of a motion to quash), 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. 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.

¹⁵³ See *supra* notes 81 and accompanying text.

¹⁵⁴ Bellia, *supra* note 35.

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.¹⁵⁵ 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.

IV. CONCLUSION

Solving the *Katz* puzzle is perhaps easier than it looks: 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 underappreciated role in influencing the quality of decisional outcomes in such controversies.

¹⁵⁵ 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 HAST. L.J. 805, 807 (2003); Freiwald, *supra* note 27, at 63.