Fordham Law Review

Volume 74 | Issue 2 Article 14

2005

Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference

Daniel J. Solove

Follow this and additional works at: https://ir.lawnet.fordham.edu/flr

 Part of the Law Commons

Recommended Citation

Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747 (2005).
Available at: https://ir.lawnet.fordham.edu/flr/vol74/iss2/14

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference

Cover Page Footnote

Associate Professor, George Washington University Law School; J.D. Yale. Thanks to Orin Kerr for thoughtful comments on this paper and for being cordial under attack. Maeve Miller and Carly Grey provided helpful research assistance.

This article is available in Fordham Law Review: https://ir.lawnet.fordham.edu/flr/vol74/iss2/14

PANEL VI: THE COEXISTENCE OF PRIVACY AND SECURITY

FOURTH AMENDMENT CODIFICATION AND PROFESSOR KERR'S MISGUIDED CALL FOR JUDICIAL DEFERENCE

*Daniel J. Solove**

INTRODUCTION

Criminal procedure courses covering search and seizure rules are almost always taught by focusing on the Fourth Amendment. Yet it is becoming ever more the case that the Fourth Amendment is playing a smaller role in regulating law enforcement investigations involving information privacy. Fourth Amendment protection continues to recede from a litany of law enforcement activities, and it is being replaced by federal statutes. We are witnessing a codification of the Fourth Amendment.

This essay examines the development of Fourth Amendment codification. Few have examined this trend. Since the criminal procedure revolution of the Warren Court era, the courts have been the primary rulemakers in the field of criminal procedure. Within the past few decades, however, we have witnessed the rise of a dualist system of criminal procedure, with statutes making up a sizeable portion of the rules. This increasing codification raises several important questions: Is the legislative regime for regulating searches and seizures better than the judicial regime? Are legislatures generally more capable than courts at crafting criminal procedure rules in the information age? How should courts apply the Fourth Amendment in a realm where increasingly they are no longer the only rulemaker?

In his provocative article, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, Professor Orin Kerr examines the rise of the statutory regime of criminal procedure when new technologies are involved.[1] Kerr goes on to argue that "courts

* Associate Professor, George Washington University Law School; J.D. Yale. Thanks to Orin Kerr for thoughtful comments on this paper and for being cordial under attack. Maeve Miller and Carly Grey provided helpful research assistance.

1. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004) [hereinafter Kerr, *Constitutional Myths*].

should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies."[2] Kerr suggests, in essence, that courts should back off and let the codification of the Fourth Amendment continue on its current course.

Kerr's focus is on new technologies, but the codification of the Fourth Amendment is expanding more broadly. The first part of this Article argues that codification has arisen in areas where courts have left a void in Fourth Amendment protection. These areas include new technologies, but they can more broadly be understood as involving issues of information privacy. Whereas courts have readily applied the Fourth Amendment for physical searches, tangible items, and actual trespasses, data presents a difficult issue, because it is often obtained in less physical ways that do not involve entering places or rummaging through things. Data often exists apart from the subject, and is frequently in the possession of others. Codification has arisen in these areas because of courts' difficulty in applying the Fourth Amendment to information—whether in high-tech form (computer searches) or low-tech form (records held by companies).

Nevertheless, Kerr's focus on technology captures a large area of the codification of the Fourth Amendment. His normative claim is that legislatures are more capable than courts of making the rules in this area.[3] It is here that Kerr's argument goes significantly astray. Certainly, the codified regime is better than no Fourth Amendment protection, and since it has arisen in areas largely left unprotected by the courts, it has filled a void. But Kerr believes that courts should allow the legislatures to take such a role, and in this regard, he seemingly endorses the trend of courts leaving areas outside of Fourth Amendment protection for legislatures to fill in with statutory rules. Kerr makes a number of contentions about why legislatures are better able to address new technologies than courts,[4] but these contentions are based on faulty assumptions that are not well grounded in either theory or practice.[5] This Article examines these legislative rules and demonstrates their deficiencies when compared to Fourth Amendment protection.

I. FROM THE CONSTITUTION TO STATUTES

Many countries regulate law enforcement primarily through a legislative or administrative regime.[6] In the United States, however, constitutional rules provide the basis for a significant number of the rules governing law enforcement investigations. In particular, three constitutional amendments

2. *Id.* at 805.
3. *Id.* at 807-08.
4. *See infra* Part II.A.
5. *See infra* Part II.A.
6. *See* Craig M. Bradley, The Failure of the Criminal Procedure Revolution 95-143 (1993).

in the Bill of Rights—the Fourth, Fifth, and Sixth Amendments—address issues of criminal procedure.[7]

A. *The Rise of the Fourth Amendment*

Beginning in the 1960s, the U.S. Supreme Court, led by Chief Justice Earl Warren, radically transformed criminal procedure. The criminal procedure revolution centered on the Fourth Amendment, which is the rule regulating what law enforcement officials can search and seize. The Fourth Amendment provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[8]

The Fourth Amendment potentially can cover a large part of the criminal investigatory process. For the Warren Court, the Fourth Amendment would become an enormous piece of the regulatory pie. To play such a role, many components of the Fourth Amendment had to come together. Piece by piece they did, with the rule reaching the pinnacle of its potential power in 1967.

First, to regulate law enforcement investigations, the Fourth Amendment required a large jurisdictional reach. The United States, unlike other countries, does not have a centralized system of policing. Rather, there are hundreds of thousands of law enforcement officials at the federal, state, and local levels.[9] For a long time, the Fourth Amendment applied only to federal officials, who have always constituted a small component of law enforcement.[10] It was not until 1949 that the Fourth Amendment was incorporated against the states in *Wolf v. Colorado*.[11]

Second, the Fourth Amendment needed a meaningful enforcement mechanism. Today, the principal remedy for a Fourth Amendment violation is the exclusionary rule. If the police violate the Fourth

---

7. The Fourth Amendment regulates police investigations. It sets forth the rules for searches and seizures, and it defines the standards and procedure for obtaining warrants. U.S. Const. amend. IV. The Fifth Amendment sets forth the rules for police questioning of suspects, grand juries, double jeopardy, and due process. U.S. Const. amend. V. The Sixth Amendment contains the rules for the right to counsel, a speedy and public trial, and an impartial jury, as well as certain rights of defendants at trial (confrontation of witnesses, compulsory process). U.S. Const. at amend. VI.

8. U.S. Const. at amend. IV.

9. According to Bureau of Justice Statistics, there are 796,518 full-time state and local law enforcement officers and 93,446 full-time federal law enforcement officials. U.S. Dep't of Justice, Bureau of Justice Statistics, http://www.ojp.usdoj.gov/bjs/lawenf.htm (last visited Sept. 14, 2005); *see also* U.S. Dep't of Justice, Bureau of Justice Statistics, http://www.ojp.usdoj.gov/bjs/fedle.htm (last visited Sept. 14, 2005).

10. Federal law enforcement officials constitute only about ten percent of law enforcement officials in the United States. *See* U.S. Dep't of Justice, Bureau of Justice Statistics, *supra* note 9.

11. 338 U.S. 25, 27-28 (1949).

Amendment, the evidence obtained by the infringement is suppressed from the defendant's criminal trial. The Court originally created the exclusionary rule in 1914, in *Weeks v. United States*,[12] but the rule only applied to the federal government. Even after the Fourth Amendment was incorporated against the states in 1949, its remedy—the exclusionary rule—was not. In 1961, in *Mapp v. Ohio*,[13] the Court finally held that the exclusionary rule applied to the states.

The third and final component of the Fourth Amendment that was necessary for it to perform the regulatory role the Warren Court envisioned was the scope of its applicability. "Applicability" refers to those particular law enforcement activities that the Fourth Amendment covers. The Fourth Amendment applies to a law enforcement activity whenever there is a "search" or a "seizure."[14] If the Fourth Amendment applies, then it requires that the search or seizure be "reasonable,"[15] which in many circumstances means that law enforcement officials must first obtain a warrant supported by probable cause. There are, of course, many instances when the Fourth Amendment does not require a warrant or probable cause. In all cases, however, the Fourth Amendment requires that the search or seizure be "reasonable." If the Fourth Amendment does not apply to a particular law enforcement activity, then it does not require any limitations on that activity.

The problem facing the Warren Court was that, under existing interpretations, the Fourth Amendment had limited applicability. In 1928, in *Olmstead v. United States*,[16] the Court concluded that wiretapping did not trigger Fourth Amendment protections because the government did not trespass inside a person's home: "The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[17] Under this interpretation, the Fourth Amendment protected a person's home from being intruded upon by government officials, a person's letters from being opened, and a person's papers from being seized.[18] The *Olmstead* Court understood privacy violations as physical intrusions. Therefore, the wiretapping in *Olmstead* did not implicate privacy concerns because the government did not trespass into the home.

In 1967, the Warren Court reversed *Olmstead* in *Katz v. United States*.[19] *Katz* appeared to indicate a profound shift in Fourth Amendment analysis.

12. 232 U.S. 383 (1914).
13. 367 U.S. 643 (1961).
14. *See* U.S. Const. amend. IV.
15. *See* U.S. Const. amend. IV.
16. 277 U.S. 438 (1928).
17. *Id.* at 464.
18. *See* Boyd v. United States, 116 U.S. 616 (1886) (holding that one's personal papers and documents were protected by the Fourth Amendment); *Ex Parte* Jackson, 96 U.S. 717 (1877) (holding that sealed letters were protected by the Fourth Amendment).
19. 389 U.S. 347 (1967).

Whereas the Court had previously applied the Fourth Amendment only in instances involving physical trespasses or the rummaging through of possessions or documents, the *Katz* Court boldly eliminated these tangible boundaries:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[20]

The Court's current approach to applying the Fourth Amendment emerges from a concurring opinion by Justice John Harlan in *Katz*, who stated that applicability of the Fourth Amendment should turn on whether (1) a person exhibits an "actual (subjective) expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[21] At least in theory, Fourth Amendment applicability can be quite broad—indeed, it can apply whenever there is a reasonable expectation of privacy.

In 1967, with these three components in place—jurisdiction encompassing all law enforcement officials, a powerful enforcement mechanism, and a broad scope of applicability—the Fourth Amendment was poised to become the primary rule to regulate law enforcement investigations. Conventional wisdom has it that the Fourth Amendment did achieve such a role—although perhaps only in potential, for no sooner than all three components were in place, the Fourth Amendment began its decline.

B. *The Decline of the Fourth Amendment*

Katz purported to usher in a wide scope of Fourth Amendment coverage based on a broad understanding of privacy. Instead of expanding its understanding of privacy, however, the Court merely shifted its view, conceiving of privacy as a form of total secrecy—a conception I have referred to as the "secrecy paradigm."[22] Under this view, a privacy invasion only occurs if a deep secret is uncovered. Therefore, if somebody could conceivably have peeked in on a person's property or if a person revealed information to another, there can be no expectation of privacy.

In a series of cases from 1983-1989, the Court held that visual or video surveillance in public falls outside of the protection of the Fourth Amendment. The police can fly above one's home and inspect one's

20. *Id.* at 351-52 (citations omitted).
21. *Id.* at 361 (Harlan, J., concurring).
22. *See* Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 42 (2004) [hereinafter Solove, Digital Person].

backyard or even any structures that have openings in their roofs.[23] The police can use sensory enhancement technology to magnify images that are exposed to the public, even if they could not detect them with the naked eye.[24] The Court also concluded that a physical tracking device that monitored the movements of a person in public was not covered by the Fourth Amendment.[25] According to the Court, a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[26]

Another limitation in Fourth Amendment applicability is the "third party doctrine," which provides that, if information is possessed or known by third parties, then a person has no reasonable expectation of privacy regarding such information.[27] For example, in 1976, in *United States v. Miller*,[28] federal law enforcement officials sought a person's financial records by subpoenaing them from his bank.[29] The banks turned over the information.[30] The bank customer argued that the Fourth Amendment applied to his records and that the government needed a search warrant to obtain them.[31] The Court, however, disagreed, and concluded that the Fourth Amendment did not apply because the customer lacked a reasonable expectation of privacy in his bank records.[32] According to the Court's reasoning, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[33] Furthermore, the Court reasoned that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[34]

Three years later, in 1979, the Court held in *Smith v. Maryland*[35] that the Fourth Amendment did not apply to pen registers—devices that recorded the phone numbers a person dialed. Because these devices were installed at the phone company, rather than inside a person's home, and because people "know that they must convey numerical information to the phone

23. Florida v. Riley, 488 U.S. 445 (1989) (upholding a helicopter inspection of a greenhouse missing a few roof panels from a helicopter); California v. Ciraolo, 476 U.S. 207 (1986) (upholding a flyover inspection of a backyard from a flyover).

24. Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

25. United States v. Knotts, 460 U.S. 276, 281-82 (1983).

26. *Id.* at 281.

27. *See generally* Computer Crime and Intellectual Prop. Section, U.S. Dep't of Justice, Manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations § I.B.3 (2001), *available at* http://www.cybercrime.gov/sdsmanual2002.htm [hereinafter DOJ Manual] (written by Orin Kerr).

28. 425 U.S. 435 (1976).

29. *Id.* at 437-38.

30. *Id.* at 438.

31. *Id.* at 438-39.

32. *Id.* at 441-43.

33. *Id.* at 443.

34. *Id.* at 442.

35. 442 U.S. 735 (1979).

company," they cannot "harbor any general expectation that the numbers they dial will remain secret."[36]

The third party doctrine presents one of the most serious threats to privacy in the digital age. Today, a multitude of companies have records of personal information. Internet service providers ("ISPs") have information that connects a person's identity to pseudonymous postings on the Internet. Bookstores and merchants such as Amazon.com keep extensive records of every purchase a person makes. The government no longer needs to enter a person's home to see what they have bought—it can get the data from the records of the companies that sold them the items. The government can find out whom a person has been talking to by examining ISP records and phone records. In the Information Age, so much of what we do is recorded by third parties that the Court's third party doctrine increasingly renders the Fourth Amendment ineffective in protecting people's privacy against government information gathering.[37]

How should the decline of the Fourth Amendment be understood? One part of the explanation is that the Supreme Court has been backing away from the Warren Court's criminal procedure revolution, as the Court today is far more conservative than the Warren Court. But the Court's narrow scope of Fourth Amendment protection can also be understood as being rooted in a flawed conception of privacy. The Court has moved from one impoverished understanding of privacy to another. Back in the days of *Olmstead,* the Court viewed privacy in terms of physical invasions—for example, probing baggage and searching homes and tangible things.[38] *Katz* recognized that, as in the case of wiretapping, a person's privacy could be invaded even though there was not an actual physical invasion. But the Court then latched onto another conception of privacy—the secrecy paradigm—which has proven to be equally, if not more, restrictive than the Court's conception of privacy in *Olmstead.*

C. *The Rise of the Statutes*

Enter Congress. The rules regulating government investigations have increasingly been those of federal statutes, not Fourth Amendment law.

---

36. *Id.* at 743.

37. *See* Solove, Digital Person, *supra* note 22, at 200-03. Because so many investigatory technologies, tools, and techniques fall outside the scope of the Fourth Amendment, commentators have long lamented the waning of Fourth Amendment protection. Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment,* 72 Miss. L.J. 5, 49 (2002); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance,* 86 Minn. L. Rev. 1325, 1326 (2002); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance,* 86 Minn. L. Rev. 1393, 1411 (2002); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions,* 65 Law & Contemp. Probs. 125, 130-33 (2002). For more articles, see Kerr, *Constitutional Myths, supra* note 1, at 802, 803 & n.7.

38. *See supra* notes 16-19 and accompanying text.

Although the third party doctrine eliminated Fourth Amendment protection from a wide range of government information-gathering activities, numerous federal statutes now fill the void. Wiretapping, for example, despite being covered by the Fourth Amendment, is largely regulated through the Wiretap Act.[39]

Some of the federal statutes were enacted in response to the Court's failure to apply the Fourth Amendment to particular situations.[40] Other statues were primarily enacted to protect consumer privacy and regulate various businesses, but they also contain provisions for government access to records and personal information.[41] A brief tour of these statutes demonstrates that they are far from a trivial part of criminal procedure. Indeed, statutory law is becoming increasingly relevant in the Information Age.

1. Electronic Surveillance Law

In most circumstances, statutes have filled the gaps left by the Fourth Amendment. The Wiretap Act, however, is one of the rare statutes that regulates in an area that the Court has found to be within the scope of Fourth Amendment protection. The original version of the Wiretap Act was enacted as Title III of the Omnibus Crime Control and Safe Streets Act in 1968.[42] This was one year after *Katz* had concluded that the Fourth Amendment applied to wiretapping[43] and *Berger v. New York* had set forth the constitutional requirements for wiretapping.[44] *Berger* and *Katz* were used "as a guide in drafting Title III."[45]

The Wiretap Act has all but supplanted the Fourth Amendment in regulating wiretaps, because the protections of the Wiretap Act exceed those of the Fourth Amendment in many circumstances. For example, unlike the Fourth Amendment, the Wiretap Act's applicability does not hinge upon a reasonable expectation of privacy.[46] Furthermore, while the Fourth Amendment only applies to government officials, the Wiretap Act applies to government officials as well as to private parties.[47] Warrants under the Wiretap Act have certain protections that Fourth Amendment warrants lack, and Orin Kerr aptly refers to Wiretap Act warrants as

39. 18 U.S.C. §§ 2510-2520 (2000); *see also infra* notes 42-50 and accompanying text.
40. *See infra* notes 52-78 and accompanying text.
41. *See infra* Part II.C.2.
42. Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520).
43. Katz v. United States, 389 U.S. 347 (1967); *see also supra* notes 19-21 and accompanying text.
44. Berger v. New York, 388 U.S. 41, 58-60 (1967) (stating that wiretap orders must particularly describe the kinds of conversations sought to be overhead and must have a termination date).
45. S. Rep. No. 90-1097, at 214-18 (1969).
46. *See generally* 18 U.S.C. §§ 2510-2511.
47. *Id.* § 2511(1).

"'super' search warrant[s]."[48] For example, beyond requiring probable cause, they require a finding that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[49] Only certain high-ranking government officials are permitted to apply for warrants under the Wiretap Act.[50]

The Stored Communications Act protects communications stored by third parties, including ISP records. The Stored Communications Act was enacted as part of the Electronic Communications Privacy Act ("ECPA") of 1986.[51] The Supreme Court has never addressed the issue of whether a person has a reasonable expectation of privacy in e-mail stored with third parties, or in subscriber information stored with an ISP. There is an argument that this information, because it is maintained by a third party, would fall under the third party doctrine.[52] The Stored Communications Act protects unread e-mail awaiting download by the user that is temporarily stored at one's ISP.[53] In addition, the government must obtain a warrant to acquire communications stored for 180 days or less.[54] After 180 days, however, the protection drops to a mere subpoena or court order.[55]

The Stored Communications Act also regulates ISP customer records. ISP records contain information that links a customer's screen name (online pseudonym) with her real identity. These records also include Internet session times, addresses, phone numbers, and billing data.[56] To obtain ISP records, the government needs to secure a court order under the Stored Communications Act, which does not require a showing of probable cause.[57] Rather, the government only has to demonstrate "specific and articulable facts showing that there are reasonable grounds" to believe communications are "relevant" to the criminal investigation.[58] The Stored Communications Act does not have an exclusionary rule.[59]

The Pen Register Act regulates government access to pen registers and trap and trace devices,[60] which, in *Smith v. Maryland*, the Supreme Court

48. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 621 (2003) [hereinafter Kerr, *Big Brother*].
49. 18 U.S.C. § 2518(3)(c).
50. *Id.* § 2516.
51. *Id.* §§ 2510-2522.
52. *See generally supra* notes 27-37 and accompanying text.
53. 18 U.S.C. § 2510(17).
54. *Id.* § 2703(a).
55. *Id.* § 2703(b).
56. *Id.* § 2703(c)(1)(C).
57. *Id.* § 2703(c)(1)(B)(ii).
58. *Id.* § 2703(d). If the government does not want to provide prior notice to the subscriber that it is seeking the information, it must obtain a warrant. *Id.* § 2703(b). However, in a number of circumstances, notice can be delayed for up to three months after information has been obtained. *Id.* § 2705.
59. United States v. Kennedy, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999).
60. 18 U.S.C. §§ 3121-3124.

held are outside the coverage of the Fourth Amendment.[61] Under the Pen Register Act, the government must obtain a court order to use a pen register or trap and trace device.[62] However, a court order differs significantly from a search warrant. The order requires that the government certify that "the information likely to be obtained by such installation and use is relevant to an ongoing investigation."[63] This standard falls well short of probable cause, as relevance is much easier to establish. Moreover, courts have no discretion; when government officials make the certification, the order must be granted.[64] There is no exclusionary rule under the Pen Register Act.

Congress has also regulated foreign intelligence surveillance. In 1972, the Supreme Court held that the Fourth Amendment standard for national security intelligence remained an open question. In *United States v. United States District Court,*[65] a case that has become known as the "*Keith* case," the Court ruled that, although surveillance for domestic criminal law enforcement was protected by ordinary Fourth Amendment rules, "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[66] The Court also noted that "[d]ifferent standards" other than a warrant "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."[67] Moreover, the Court explicitly left open the question of the surveillance of "foreign powers," opining that warrantless surveillance under these limited circumstances "may be constitutional."[68]

Keith left more questions than answers. In part to fill the gaps left by *Keith,* Congress passed the Foreign Intelligence Surveillance Act ("FISA") of 1978.[69] FISA's purpose is to create a regulatory regime for foreign intelligence gathering.[70] FISA creates a secret court of eleven judges to issue court orders for government foreign intelligence-gathering activities.[71]

---

61. Smith v. Maryland, 442 U.S. 735 (1979).
62. 18 U.S.C. § 3121(a).
63. *Id.*
64. *Id.* § 3123(a)(1).
65. 407 U.S. 297 (1972).
66. *Id.* at 322.
67. *Id.* at 322-23.
68. *Id.* at 322 n.20.
69. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-1811 (2000)).
70. The purpose of the Foreign Intelligence Surveillance Act ("FISA") was to erect a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S. Rep. No. 604 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3916.
71. Originally, there were seven judges on the court, but the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act ("USA-PATRIOT Act") raised the number to eleven. *See* USA-PATRIOT Act, Pub. L. No. 107-56, § 208(i), 115 Stat. 272, 283 (2001) (to be codified at 50 U.S.C. § 1803(a)). For

FISA orders are granted if there is probable cause to believe that the monitored party is a "foreign power" or "an agent of a foreign power."[72] Evidence obtained under a FISA order can be used in a regular criminal prosecution.[73]

Very soon after the September 11, 2001, terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act ("USA-PATRIOT Act") of 2001.[74] The USA-PATRIOT Act made a number of changes to the federal statutes discussed above. It expanded the definition of pen registers from "numbers dialed . . . on the telephone line" to all "dialing, routing, addressing, or signaling information."[75] This expansion means that the Pen Register Act now covers the addressing information on e-mails, Internet Protocol addresses ("IP addresses"), and Uniform Resource Locators ("URLs").

The USA-PATRIOT Act also expanded the information that could be obtained under the Stored Communications Act, adding "records of session times and durations," "any temporarily assigned network address," and "any credit card or bank account number" used for payment.[76] Moreover, the USA-PATRIOT Act expanded the scope of FISA. FISA originally applied only when "the purpose" of the investigation was to gather foreign intelligence.[77] This limited FISA's scope to when the primary purpose of an investigation was foreign intelligence gathering. FISA now applies whenever foreign intelligence gathering is "a significant purpose" of the investigation.[78] This means that foreign intelligence gathering only needs to be one of the goals of an investigation, thereby allowing the government to use FISA to obtain information for criminal prosecution purposes.

2. Regulation of Government Access to Records

In the void left by the third party doctrine, Congress has established a regime to regulate government access to records. Such a regime has been constructed piecemeal. Many of the provisions that address law enforcement access appear in various statutes that primarily deal with consumer and financial privacy, and are not primarily devoted to law enforcement issues.

In 1978, two years after the Supreme Court concluded in *United States v. Miller* that the Fourth Amendment did not cover bank records, Congress

---

more details about the workings of the Foreign Intelligence Surveillance Court ("FISC"), see Benjamin Wittes, *Inside America's Most Secretive Court,* 143 N.J. L.J. 777 (1996).

72. 50 U.S.C. § 1805(a)(3)(A) (2000).

73. *Id.* § 1806(b).

74. Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified at 50 U.S.C. §§ 1801-62).

75. 18 U.S.C. § 3127(3) (2000), *amended by* USA-PATRIOT Act § 216, 18 U.S.C.A. § 3127(3) (West 2005).

76. 18 U.S.C.A. § 2703(c)(2).

77. 50 U.S.C. § 1805(a)(3)(A).

78. 50 U.S.C. § 1804(a)(7)(B), *amended by* USA-PATRIOT Act § 204, 18 U.S.C.A. § 1804(a)(7)(B).

responded by passing the Right to Financial Privacy Act ("RFPA").[79] The RFPA requires the government to use a subpoena to access financial information.[80] The subpoena requires a "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."[81] People must be given prior notice of the subpoena so they can challenge it in court; however, in many circumstances, the government can delay notice.[82]

The Fair Credit Reporting Act ("FCRA") of 1970, although primarily a consumer privacy protection statute, contains provisions regarding law enforcement access to credit records.[83] Credit reporting agencies maintain detailed records on nearly every American citizen. These records include not only financial information, but also data about people's lifestyles, spending habits, and anything else relevant to creditors.[84] Under the FCRA, a consumer reporting agency "may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, and former places of employment, to a governmental agency."[85] When the government wants to obtain other information, it must seek a court order or grand jury subpoena.[86] Furthermore, the Federal Bureau of Investigation ("FBI") can request a list of all financial institutions where a person maintains an account.[87]

The Family Education Right to Privacy Act ("FERPA") of 1974 protects the privacy of school records, which can include extensive information about students.[88] Law enforcement officials may obtain these records "pursuant to any lawfully issued subpoena."[89]

The Cable Communications Policy Act ("CCPA") of 1984, which regulates the privacy of a person's records with her cable television company, is another statute designed to protect consumer privacy.[90] Like many others, the CCPA also contains a provision for law enforcement access to cable records.[91] The government must establish "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought

79. Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630, 92 Stat. 3641 (1978) (codified as amended at 12 U.S.C. §§ 3401-3422 (2000)).

80. *See* 12 U.S.C. §§ 3401-3422. For more information on the Right to Financial Privacy ("RFPA"), see George B. Trubow & Dennis L. Hudson, *The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion*, 12 J. Marshall J. Prac. & Proc. 487 (1979).

81. 12 U.S.C. § 3407.

82. *Id.* § 3409.

83. 15 U.S.C. § 1681 (2000).

84. Solove, Digital Person, *supra* note 22, at 21.

85. 15 U.S.C. § 1681f.

86. *Id.* § 1681b(a)(1).

87. *Id.* § 1681u.

88. 20 U.S.C. § 1232g (2000).

89. *Id.* § 1232g(b)(2)(B).

90. 47 U.S.C. § 551 (2000).

91. *Id.* § 551(h).

would be material evidence in the case."[92] People can "appear and contest" the court order.[93] There is, however, no exclusionary rule under the CCPA.

The Video Privacy Protection Act ("VPPA") of 1988,[94] primarily a consumer privacy statute, enables law enforcement officials to obtain a person's videotape rental records from her video store pursuant to a grand jury subpoena or court order.[95] Similarly, the regulations promulgated under the Health Insurance Portability and Accountability Act ("HIPAA") of 1996[96] permit law enforcement officials to access medical records with a court order or subpoena.[97] Law enforcement officials need only ask for the information "for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person."[98]

3. Searches Involving Communicative Material

Congress has also regulated searches involving communicative material, such as documents used for the purpose of engaging in journalism or public communication, as well as correspondence and letters in the mail. In 1978, in *Zurcher v. Stanford Daily*,[99] police searched the offices of a newspaper to find photographs of people involved in a demonstration.[100] The newspaper was not involved in the demonstration and was not suspected of criminal activity.[101] The Court concluded that the law enforcement officials could conduct the search if the officials had probable cause to believe that evidence of a crime would be located at the property.[102] The Court concluded that the requirements of a warrant "should afford sufficient protection" against these harms.[103]

In response to *Zurcher,* Congress passed the Privacy Protection Act ("PPA") of 1980.[104] The PPA restricts the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication."[105] The PPA requires that the government obtain a subpoena for work product materials, allowing the opposing party to challenge the request in court and to produce the requested documents without having the police search the premises.

---

92. *Id.* § 551(h)(1).
93. *Id.* § 551(h)(2).
94. 18 U.S.C. § 2701 (2000).
95. *Id.* § 2710(b)(2)(C).
96. 29 U.S.C. §§ 1181-1183, 42 U.S.C. § 300gg (2000); *see* 45 C.F.R. § 160-64 (2004).
97. 45 C.F.R. § 164.512(f)(1)(ii)(A).
98. *Id.* § 164.512(f)(2).
99. 436 U.S. 547 (1978).
100. *Id.* at 551.
101. *Id.*
102. *Id.* at 554.
103. *Id.* at 565.
104. Pub. L. No. 96-440, 94 Stat. 1879 (1980) (codified as amended at 42 U.S.C. § 2000aa (2000)).
105. 42 U.S.C. § 2000aa(a).

Statutory law also regulates the search and seizure of postal mail.[106] In this area, the Supreme Court in 1877 held that the Fourth Amendment requires a search warrant in order for law enforcement officials to open letters and parcels.[107] A federal statute overlaps with this holding, requiring a search warrant before law enforcement officials can open a letter.[108]

II. CONGRESS VERSUS THE COURTS

The previous part demonstrated that, for a significant portion of criminal investigations, especially those involving information, a regime of federal statutes—rather than the Fourth Amendment—governs. Orin Kerr is one of the few to have analyzed the implications of this profound shift from constitutional to statutory regulation of government investigations.[109] Kerr contends that legislative rules are in many respects preferable to judicial ones, and he goes on to argue that "the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing."[110] Legislatures, according to Kerr, "offer significant institutional advantages over courts."[111] Accordingly, "[c]ourts should recognize their institutional limitations and remain cautious until the relevant technology and its applications stabilize."[112]

What does Kerr mean by invoking the language of judicial "caution"? The language is that of deference, which is also referred to as judicial restraint. Elsewhere, I have critiqued the underpinnings used to justify judicial deference, concluding that "[d]eference is the negation of critical inquiry."[113] Kerr is unclear in his article about what precisely judges should do when faced with applying the Fourth Amendment to a new technology. One interpretation of Kerr's call for "caution" is for judges to be more reluctant to find the Fourth Amendment applicable to new technologies—in other words, to conclude that, when law enforcement activities involve new technologies, they fall outside of the Fourth Amendment's protection. Because Fourth Amendment applicability turns on whether or not there is a reasonable expectation of privacy, perhaps Kerr is suggesting that courts should be reluctant to find a reasonable expectation of privacy. As Kerr notes, "[j]udicial deference has often invited Congressional regulation."[114] Therefore, the most deferential position

106. 39 U.S.C. § 3623(d) (2000).
107. *Ex Parte* Jackson, 96 U.S. 727 (1877).
108. 39 U.S.C. § 3623(d).
109. Kerr, *Constitutional Myths, supra* note 1, at 807.
110. *Id.* at 806; *see also* Jeffrey Rosen, The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age 210-11 (2004) ("Congress is better suited than the courts to strike a reasonable balance between liberty and security") (discussing Kerr's thesis).
111. Kerr, *Constitutional Myths, supra* note 1, at 807-08.
112. *Id.* at 808.
113. Daniel J. Solove, *The Darkest Domain: Deference, Judicial Review, and the Bill of Rights*, 84 Iowa L. Rev. 941, 1020 (1999) [hereinafter Solove, *The Darkest Domain*].
114. Kerr, *Constitutional Myths, supra* note 1, at 806.

courts can take is simply to hold that the Fourth Amendment does not apply, and allow Congress to fill the void.

The question becomes the following: Should courts be more bold in expanding the scope of the Fourth Amendment to encompass new technologies? Or should courts cautiously hold off and allow legislatures to craft the regulation? The next part of this Article argues that Kerr is too quick to extol the virtues of Congress and that he is especially misguided in suggesting that courts take a back seat to legislatures in creating criminal procedure rules for new technologies.

A. *Are Legislative Rules Better than Judicial Rules?*

Kerr makes a number of arguments in support of his call for judicial restraint. Kerr's key contentions are that (1) legislatures create rules that are more comprehensive, balanced, clear, and flexible; (2) legislatures are better able to keep up with technological change; and (3) legislatures are more adept at understanding complex new technologies.[115] The following sections examine each contention in turn.

1. Creating a Comprehensive and Balanced Set of Rules

Kerr argues that a key goal in drafting criminal procedure rules is to create "a rule-structure that simultaneously respects privacy interests and law enforcement needs."[116] According to Kerr, unlike courts, "[l]egislatures can enact comprehensive rules based on expert input and can update them frequently as technology changes."[117] Moreover, legislative rules "are more nuanced, clear, and . . . optimize the critical balance between privacy and public safety more effectively when technology is in flux."[118]

However, there seems to be no reason why a statutory regime will inevitably be any more comprehensive, balanced, or clear than a regime based on Fourth Amendment principles. When the Fourth Amendment covers a particular law enforcement activity, it provides a set of rules to regulate it. Once a law enforcement activity falls within the Fourth Amendment's regulatory regime, courts will examine whether the search or seizure was "reasonable."[119] A search with a warrant supported by probable cause is generally reasonable. Only on very rare occasions are

115. Specifically, he argues as follows: "When technologies are new and their impact remains uncertain, statutory rules governing law enforcement powers will tend to be more sophisticated, comprehensive, forward-thinking, and flexible than rules created by the judicial branch." *Id.* at 859-60.

116. *Id.* at 861.

117. *Id.* at 807.

118. *Id.* at 806.

119. *See* U.S. Const. amend. IV.

searches pursuant to a valid warrant unreasonable.[120] A search without a valid warrant is often deemed unreasonable. This is known as the "per se warrant rule."[121]

Warrants are a judicial authorization for a particular search. Warrants must be supported by probable cause, which exists when there is "reasonably trustworthy information" that the search will turn up evidence of a crime.[122] The purpose of a warrant is to have an independent party (judges or magistrates) ensure that government officials really do have probable cause to conduct a search.

Kerr criticizes the Fourth Amendment rules as inflexible, but in reality they show a remarkable degree of flexibility. First, the warrant requirement balances privacy interests and law enforcement needs by allowing searches and seizures to occur only after law enforcement officials justify them before a judge or magistrate.

Second, in situations where warrants and probable cause do not work well, the Court has made exceptions. Indeed, there are numerous exceptions to the warrant and probable cause requirements, such as *Terry* stops, exigent circumstances, and "special needs" in schools and workplaces.[123] These exceptions allow the courts to accommodate a wide range of government investigative activity within the protective framework of the Fourth Amendment.

In contrast, the statutory regime that Kerr extols has many deficiencies that caution against Kerr's enthusiasm for legislative rules. When the statutes are examined as a whole—as an alternative regulatory regime to the Fourth Amendment—there are many severe problems that refute Kerr's belief in the superiority of a legislative regime.[124]

---

120. *See* Winston v. Lee, 470 U.S. 753 (1985) (operating on the defendant to retrieve a bullet inside his body was an unreasonable search, even though there was a valid warrant for it).

121. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1118 (2002) [hereinafter Solove, *Digital Dossiers*].

122. Brinegar v. United States, 338 U.S. 160, 175-76 (1949) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)).

123. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 719-20 (1987) (holding that, when a government employer conducts a warrantless search, a court "must balance the invasion of the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace"); New Jersey v. T.L.O., 469 U.S. 325, 340 (1984) (stating that a warrant requirement is unsuited to the school environment, despite children's expectations of privacy); Terry v. Ohio, 392 U.S. 1, 21 (1968) (holding that an investigatory stop without a warrant is justified when a police officer is "able to point to specific and articulable facts which . . . reasonably warrant that intrusion").

124. In his reply, Kerr contends that I unfairly pit an idealized Fourth Amendment regime against the statutory regime. In other words, I am comparing a Fourth Amendment regime as if the courts had applied the Fourth Amendment to various new technologies against the statutory regime as is. But Kerr's contention is normative and proscriptive in that he recommends that going forward, legislatures, and not courts, should be the primary rulemakers. He criticizes scholars who call for the courts to expand Fourth Amendment applicability. The current status quo reveals areas where the courts refused to apply the Fourth Amendment and where legislatures became involved. I aim to ask, are we better off

First, Congress's statutes lack effective remedies because the federal statutes often lack exclusionary rules. For example, there is no exclusionary rule to protect e-mail under the Wiretap Act,[125] and the Stored Communications Act and Pen Register Act both lack an exclusionary rule.[126] Kerr, in fact, wrote an article lamenting exactly this fact.[127] Most of the statutes regulating law enforcement access to records held by third parties also lack an exclusionary rule.[128] As a result, there is often little incentive for criminal defendants to challenge violations of these statutes.

Second, there are many gaps in the statutes. Consider electronic surveillance law, for example. The Wiretap Act fails to cover silent video surveillance.[129] As one court observed,

> Television surveillance is identical in its indiscriminate character to wiretapping and bugging. It is even more invasive of privacy, just as a strip search is more invasive than a pat-down search, but it is not more indiscriminate: the microphone is as "dumb" as the television camera; both devices pick up anything within their electronic reach, however irrelevant to the investigation.[130]

As another court observed, "[V]ideo surveillance can be vastly more intrusive [than audio surveillance], as demonstrated by the surveillance in this case that recorded a person masturbating before the hidden camera."[131]

Beyond video surveillance, there are numerous technologies Congress has failed to regulate. Global positioning systems enable people's movements to be tracked wherever they go.[132] Facial recognition systems can enable surveillance photos and videos to be scanned to identify particular people based on their facial features.[133] Satellite technology may be used to examine practically any open area on earth.[134] Radio frequency identification ("RFID") involves tags placed into products, objects, and

---

with the void as filled by the legislative rules, or would we be better off had the Fourth Amendment been interpreted to encompass a particular law enforcement activity? I believe in many instances, the latter would be better.

125. *See* 18 U.S.C. §§ 2510-2522 (2000).

126. *See* Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2000); Pen Register Act, 18 U.S.C. §§ 3121-3127 (2000).

127. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805 (2003) [hereinafter Kerr, *Fog*].

128. *See generally supra* notes 78-98 and accompanying text.

129. *See, e.g.*, United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 539 (9th Cir. 1992); United States v. Biasucci, 786 F.2d 504, 508 (2d Cir. 1986).

130. United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984) (emphasis omitted).

131. United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990).

132. Brendan I. Koerner, *Spy Games: From Black Boxes to GPS Devices, Your Car is Recording Your Every Move*, Reader's Dig., July 2004, at 80.

133. Daniel J. Solove & Marc Rotenberg, Information Privacy Law 313 (2003).

134. *See* Mark Monmonier, Spying with Maps: Surveillance Technology and the Future of Privacy (2002).

even human beings that emit a decipherable signal.[135] As this technology develops and tags can be read at greater distances, RFID might be used to track people's movements.

Congress has not passed statutes to address the privacy implications of any of these technologies. Nor has Congress passed a law to regulate video surveillance of citizens. Ironically, FISA regulates video surveillance, but the ECPA does not,[136] meaning that the video surveillance of a foreign spy receives more federal statutory protection than that of a U.S. citizen.[137] Nor has Congress regulated the use of tracking devices, key logging devices, or other new technologies.

Kerr critiques the Supreme Court's ruling in *Kyllo v. United States*[138] as the exemplar of the shortcomings of judicial rules for regulating technology.[139] *Kyllo* involved the use of thermal sensors by law enforcement officials to detect marijuana heat lamps inside a person's home.[140] The Court held that the Fourth Amendment required a search warrant before using such devices to detect activities inside a person's home.[141] Kerr argues that "the [*Kyllo*] opinion captures the prevailing *zeitgeist* about law, technology, and privacy. When technology threatens privacy, the thinking goes, the courts and the Constitution should offer the primary response."[142]

Kyllo sets forth the Court's current approach to analyzing sensory enhancement technology: When the technology is not in general public use and is used to detect activities in the home, a warrant is required.[143] This does leave open many questions: What happens when technology enters general public use? What about uses beyond the home?

Certainly, *Kyllo* has problems in articulating a clear approach to when sensory enhancement technology can be employed. But was Congress any better? Congress has never passed a law addressing sensory enhancement technologies, despite having had a long time to do so. Back in 1986, the Supreme Court held in *Dow Chemical Co. v. United States*[144] that the

135. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2060 (2004); Jonathan Krim, *Embedding Their Hopes in RFID: Tagging Technology Promises Efficiency but Raises Privacy Issue*, Wash. Post, June 23, 2004, at E1.

136. 18 U.S.C. §§ 2510-2522 (2000).

137. FISA requires that the government submit "a detailed description of the nature of the information sought and the type of communication or activities to be subjected to the surveillance" and a certification "that such information cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804(a)(6)-(7) (2000). For cases holding that the Electronic Communications Privacy Act ("ECPA") does not cover silent video surveillance, see *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994), *United States v. Koyomejian*, 970 F.2d 536, 539 (9th Cir. 1992), and *United States v. Biasucci*, 786 F.2d 504, 508 (2d Cir. 1986).

138. 533 U.S. 27 (2001).

139. Kerr, *Constitutional Myths, supra* note 1, at 802.

140. *Kyllo*, 533 U.S. at 29.

141. *Id.* at 40.

142. Kerr, *Constitutional Myths, supra* note 1, at 802.

143. *Kyllo*, 533 U.S. at 40.

144. 476 U.S. 227, 238 (1986).

Fourth Amendment did not apply to highly magnified photographs taken from a high-tech aerial camera at very high altitudes. The Court reasoned as follows: "The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[145] The *Dow Chemical* case raised a host of questions about what limits, if any, should be placed on sensory enhancement technology. The Court cautiously refused to impose a rule to regulate such technologies. Congress could have responded with legislation, but it did not. There is little reason, therefore, to assume that if the courts hold that the Fourth Amendment is inapplicable to a new technology, Congress will swoop in and save the day.

Beyond electronic surveillance law, the law regulating government access to records held by third parties also has tremendous gaps. Although the RFPA and the FCRA regulate government access to financial data,[146] there are many situations where financial data is unprotected, such as when the information is held by employers, landlords, merchants, creditors, database companies, and others.[147] HIPAA regulates access to medical records, but only when in the hands of certain third parties (doctors, hospitals, insurers, and so on).[148] Medical websites containing people's personal information are not covered by HIPAA.[149] Basically, the problem is that the statutes focus on who is holding the information, rather than on the information itself. Thus, the same piece of information can be protected if held by one third party and completely unprotected if held by a different third party. Some third parties that have extensive information about individuals are not covered at all, including bookstores, merchants, restaurants, employers, and other businesses. There are numerous database companies that compile extensive dossiers on individuals, yet existing statutes often do not cover law enforcement access to this data.

Second, beyond enormous gaps in protection, the statutes offer far less protection than the Fourth Amendment. Most permit law enforcement access to information based only on a court order or subpoena, rather than on a warrant.[150] Prosecutors, not judges, issue the subpoenas.[151] Professor William Stuntz observed as follows: "[W]hile searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably

145. *Id.* at 228.

146. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2000); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t (2000).

147. *See* Solove, Digital Person, *supra* note 22, at 206.

148. Doctors, hospitals, and insurers are "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA") regulations, and therefore the rules apply to them. 45 C.F.R. § 160.102 (2004).

149. Pew Internet & Am. Life Project, Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users 7 (2001), *available at* http://pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf.

150. *See* Solove, Digital Person, *supra* note 22, at 202-09; *see also* Daniel J. Solove, *Data Privacy and the Vanishing Fourth Amendment*, Champion Mag., May 2005, at 20.

151. Louis Fisher, *Congress and the Fourth Amendment*, 21 Ga. L. Rev. 107, 152 (1986).

burdensome to its target. Few burdens are deemed unreasonable."[152] The court orders required by the statutes also require far less than probable cause. Typically, mere "relevance" to an ongoing criminal investigation is all that such statutes require.[153]

Thus, in areas where the courts have backed off and left a void that Congress has attempted to fill, the statutes have not, in large part, measured up. Given a choice, it seems that a better balance between privacy interests and law enforcement needs could have been reached if the courts had held that the Fourth Amendment covered a particular law enforcement activity. Thus, we could have the courts take Kerr's advice and exercise caution and restraint, allowing Congress to craft the rules, or we could have the courts be more willing to expand the coverage of the Fourth Amendment. Where the courts have left open areas for legislative rules to fill in, Congress has created an uneven fabric of protections that is riddled with holes and that has weak protections in numerous places. Therefore, Kerr's claim that legislatures create more comprehensive and balanced rules than courts is simply not borne out by the evidence.

Another of Kerr's reasons for preferring legislatures to courts is his view that legislatures will craft clearer rules than courts. Kerr is particularly keen on avoiding unclear rules, and he lists "rule clarity" as a key goal for a criminal procedure system.[154] Kerr argues that "[u]nclear rules mean unclear limits on government power, increasing the likelihood of abuses by aggressive government officials."[155] According to Kerr, legislative rules "are more nuanced, clear, and . . . optimize the critical balance between privacy and public safety more effectively when technology is in flux."[156]

Yet the rules of the ECPA are notoriously confusing and unclear, as Kerr himself frequently points out in his writings.[157] If electronic surveillance law were clear, Kerr would have a lot less to write about. He has written countless articles seeking to explain the meaning of the electronic surveillance laws,[158] and has built his reputation as one of the few people

152. William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 Harv. L. Rev. 842, 857-58 (2000).

153. *See* Stored Communications Act, 18 U.S.C. § 2703(d) (2000) (providing that law enforcement officials can obtain Internet Service Provider ("ISP") records with "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation"); Pen Register Act, 18 U.S.C. § 3123(a) (2000) (providing that law enforcement officials can obtain pen register information if "the information likely to be obtained . . . is relevant to an ongoing criminal investigation."); Right to Financial Privacy Act, 12 U.S.C. § 3407(1) (2000) (providing that law enforcement officials can obtain financial information if they have "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry").

154. Kerr, *Constitutional Myths*, *supra* note 1, at 861.

155. *Id.*

156. *See id.* at 806.

157. *See infra* notes 160-61 and accompanying text.

158. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) [hereinafter Kerr, *User's Guide*];

on the planet who can actually make sense of the law. It is no wonder that Kerr prefers the statutes; this is his home turf. As for clarity, there are many open questions under electronic surveillance law, and many provisions subject to conflicting interpretations. Kerr really does not point us to a clearer regime; rather, he simply points us to one that he understands better.

Furthermore, federal statutes are not self-executing, meaning that they must be interpreted and applied by courts. 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.[159] A large part of the problem is that the statutory law is extremely complicated. For instance, Kerr's favorite law, the ECPA, is immensely complicated, and he notes that it is "unusually difficult to understand."[160] He also observes that the "law of electronic surveillance is famously complex, if not entirely impenetrable."[161] The problem, then, is not the Fourth Amendment, but the outdated, overly complex statutes that courts must apply.

Part of the problem with the complexity of electronic surveillance law stems from the flexibility that Kerr praises. Kerr commends Congress for dreaming up eight different kinds of "statutory thresholds" for electronic surveillance law.[162] While this certainly is more flexible, it has also led to great confusion. Kerr has painstakingly attempted to explain these different standards, which are readily confused and difficult to figure out.[163] Not only federal officials, but also local law enforcement officials, must understand these standards. Most local police officers, however, lack the benefit of having years to study the mysteries of the ECPA.

The problem is that flexibility and clarity are often in conflict. The multiple exceptions to the warrant and probable cause requirement of the Fourth Amendment, which give the Fourth Amendment rules some flexibility, have been criticized as confusing. As Silas Wasserstrom and Louis Michael Seidman observe, the per se warrant rule is "so riddled with

---

Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279 (2005); Kerr, *Big Brother*, *supra* note 48; Kerr, *Fog*, *supra* note 127.

159. *See, e.g.*, Kerr, *User's Guide*, *supra* note 158, at 1208; Kerr, *Fog*, *supra* note 127, at 807 (complaining that ECPA "remains unusually obscure" and that it "remains a fog"). Kerr decries that the Stored Communications Act "remains poorly understood. Courts, legislators, and even legal scholars have had a very hard time making sense of the [Stored Communications Act]. The statute is dense and confusing . . . ." Kerr, *User's Guide*, *supra* note 158, at 1208.

160. Kerr, *Fog*, *supra* note 127, at 820.

161. *Id.*

162. Kerr, *Constitutional Myths*, *supra* note 1, at 872.

163. Kerr, *Big Brother*, *supra* note 48, at 620-21 (creating a chart for understanding the standards).

exceptions, complexities, and contradictions that it has become a trap for the unwary."[164]

The problems of clarity and flexibility are endemic to all rules, whether legislative or judicial. An examination of the current law, however, far from revealing legislative superiority in achieving clarity and flexibility, demonstrates that both legislatures and courts are for the most part in the same boat.

2. Keeping Up with Technological Change

Kerr argues that legislatures are better able than courts to craft rules dealing with changing facts. According to Kerr, courts, unlike legislatures, "cannot update rules quickly as technology shifts."[165] Kerr argues that a key difference between legislative and judicial rules is that "legislatures typically create generally applicable rules ex ante, while courts tend to create rules ex post in a case-by-case fashion."[166] Kerr goes on to argue that "legislatures enact generalized rules for the future, whereas courts resolve disputes settling the rights of parties from a past event. The difference leads to Fourth Amendment rules that tend to lag behind parallel statutory rules and current technologies by at least a decade."[167]

The same is true, however, for the statutory law. The problem with ex ante laws is that they cannot anticipate all of the new and changing factual situations that technology brings about. Ex post rules, in contrast, are often much better tailored to specific types of technology, because such rules arise as technology changes, rather than beforehand.

Kerr points to a series of gaps in Fourth Amendment law—areas where no court has made a determination as to whether the Fourth Amendment applies to a particular technology. He observes that pen registers "were in widespread use by the 1960s, but the Supreme Court did not pass on whether their use violated the Fourth Amendment until 1979."[168] Congress, however, waited even longer, and did not spring into action until 1986.[169]

Kerr continues his argument by pointing out that "no Article III court at any level has decided whether an Internet user has a reasonable expectation of privacy in their e-mails stored with an Internet service provider; whether encryption creates a reasonable expectation of privacy; or what the Fourth Amendment implications of . . . Internet surveillance . . . might be."[170]

This is true, but has Congress addressed these topics? Congress has yet to pass a statute addressing whether law enforcement officials must obtain a warrant or court order to decode encrypted files they have seized.

---

164. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 Geo. L.J. 19, 34 (1988).

165. Kerr, *Constitutional Myths*, *supra* note 1, at 807.

166. *Id.* at 868.

167. *Id.*

168. *Id.* at 869.

169. *Id.* at 855.

170. *Id.* at 869.

Regarding privacy in e-mail, the Stored Communications Act is unclear about the level of protection provided to e-mail that is already read by the user, but left on the ISP's server.[171] Such a situation is increasing in its frequency, due to the rise of web-based e-mail systems such as Gmail, Hotmail, and Yahoo e-mail, where people's e-mail remains stored at the server and not deleted after it is read. The Department of Justice takes the position that read e-mail is "simply a remotely stored file" that can be obtained with a mere subpoena.[172] This position was articulated in a manual written by none other than Orin Kerr.[173] Many other contested questions of electronic surveillance law remain.[174]

According to Kerr, legislatures are superior to courts in these situations because legislatures "can act at any time, even when a technology is new" and "recent history suggests that legislatures usually act at a surprisingly early stage, and certainly long before the courts."[175] Such a history is haphazard at best, as there are numerous forms of technology legislatures have not acted on. Kerr does not provide any structural reason why legislatures can act earlier, or why creating a law before technology is fully understood or developed is necessarily a good thing. Often the problem with ex ante legislative rules is that technology changes afterwards.

Kerr notes that courts would need to "change the governing rules at regular intervals" in order to "allow the governing rules to change as needed over time."[176] He then states that "it's hard to imagine the courts creating new rules every few years to keep the law up to date."[177] Congress, however, has not done a good job of this, and its rules regulating electronic surveillance are hopelessly out of date. Throughout the entire twentieth century and continuing on through the present, there have been only a few times Congress has made major changes in electronic surveillance law: in 1934, 1968, 1978, 1986, and 2001.[178]

First, in 1934, Congress enacted § 605 of the Federal Communications Act[179] to regulate wiretapping six years after the Court held in *Olmstead* that the Fourth Amendment did not apply.[180] Although Kerr complains that

171. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264, 1281 (2004).

172. DOJ Manual, *supra* note 27, § III.B.

173. *See id.*

174. For an extensive discussion of numerous contested issues, ambiguities, and problems in electronic surveillance law, see Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1434-38 (2004); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 67-69 (2004); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1582-98 (2004).

175. Kerr, *Constitutional Myths*, *supra* note 1, at 870.

176. *Id.* at 873.

177. *Id.*

178. *See infra* notes 179-91 and accompanying text.

179. 6 U.S.C. § 605 (1934) (current version at 47 U.S.C. § 605 (2000)).

180. Olmstead v. United States, 277 U.S. 438 (1928); *see also supra* notes 16-18 and accompanying text.

the Court took a very long time to address wiretapping, Congress took even longer. And when it finally did address wiretapping with § 605, the law was a disaster. Dislike of § 605 was nearly universal.[181] Section 605, which governed wiretapping for longer than any other federal statute, struck a terrible balance by anyone's standards. Section 605 requires as follows: "[N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[182] Section 605 did not specify how it was to be enforced, and it took the courts to fix this ambiguity and conclude that evidence obtained in violation of the Act would be excluded from evidence in federal court.[183] The Department of Justice and the FBI interpreted § 605 to prohibit only the disclosure of evidence at trial, not the practice of wiretapping itself.[184] This enabled FBI Director J. Edgar Hoover to wiretap to his heart's content so long as he used wiretapping only to blackmail people, rather than to provide evidence in federal trials.

Second, in 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act to regulate electronic surveillance and reform the misguided regime of § 605.[185] By this time, however, the Court had already overruled *Olmstead* and had provided useful guidance to Congress about what to include in its law in *Berger*.[186]

Third, in 1978, Congress enacted FISA to regulate foreign intelligence gathering.[187] FISA created a regime distinct from that of Title III, which governed domestic surveillance.[188]

Fourth, in 1986, Congress revised Title III with the ECPA, which was Congress's most proactive legislation.[189] Although the ECPA was grand in scope, Congress has done little to modernize the ECPA in the nearly two decades since its passage.

Finally, in 2001, Congress passed the USA-PATRIOT Act.[190] Kerr trumpets the virtues of legislatures having time to explore the facts and really understand the technologies, but the USA-PATRIOT Act was rushed

181. *See* Solove, *supra* note 171, at 1274-75 ("Attorney General Nicholas Katzenback declared [§ 605] the 'worst of all possible solutions.' According to Senate Report 1097, section 605 'serves . . . neither the interests of privacy nor of law enforcement.'"); *see also* James G. Carr & Patricia L. Bellia, The Law of Electronic Surveillance § 2.1, at 2-5 (2d ed. 2004).

182. 47 U.S.C. § 605.

183. Nardone v. United States, 302 U.S. 379, 382 (1937).

184. *See* Wayne R. LaFave et al., Criminal Procedure 260 (3d ed. 2000).

185. Pub. L. No. 90-351, 82 Stat. 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000)).

186. Berger v. New York, 388 U.S. 41 (1967).

187. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-1811 (2000)); *see also supra* notes 68-73 and accompanying text.

188. *See supra* notes 68-73 and accompanying text.

189. 18 U.S.C. §§ 2510-2522.

190. Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified at 50 U.S.C. §§ 1801-62); *see also supra* notes 74-78 and accompanying text.

through Congress in great haste.[191] Moreover, without the tragic events of September 11, it is unlikely that Congress would have made any significant changes to electronic surveillance law in 2001.

This is hardly a regular updating of the law. Although the ECPA has been amended between 1986 and 2001, Kerr admits elsewhere that these "subsequent changes have merely nibbled around the edges of the law."[192] For the domestic surveillance regime, there had been a lag of thirty-four years between § 605 and Title III, eighteen years between Title III and the ECPA, and fifteen years between the ECPA and the USA-PATRIOT Act. If anything, this historical record suggests that Congress is actually far worse than the courts in reacting to new technologies. The ex ante law of the ECPA that Kerr extols now has many spots where it no longer fits the technology.[193] Since the passage of the ECPA, technology has not sat still. E-mail has flourished. The Internet has blossomed. Cyberspace has transformed our lives. Whereas at one point, before the frequent use of e-mail and the Internet, the ECPA might have been a visionary ex ante law, it has since become quite outdated.

This history should not be surprising. Indeed, it is hard to imagine Congress keeping statutes up to date. Federal legislation is not easy to pass, and it usually takes a dramatic event to spark interest in creating or updating a law. Congress often only gets involved when there is a major uproar or problem, and unless there is a strong impetus, little new lawmaking occurs. In contrast, courts must get involved every time an issue arises in a case. As a result, issues are likely to be addressed with more frequency in the courts than in Congress. Kerr has it exactly backwards.

3. Comprehending Complex Technologies

A basic premise in Kerr's reasoning is that new technologies are complex and difficult to understand, and legislatures are better equipped to deal with such complexities. Specifically, he argues that courts "lack the information needed to understand how the specific technologies in cases before them fit into the broader spectrum of changing technologies."[194]

There is no reason, however, to assume that the average legislator can better understand technology than the average judge. There may be a few in Congress with a good understanding of the technology, but many lack the foggiest idea about how new technologies work.

Moreover, in many cases, the technologies at issue are not particularly complex. Do we really need two years and thousands of pages of detailed information to understand how e-mail works? If understanding e-mail

191. *See* Beryl A. Howell, *Seven Weeks: The Making of the USA-PATRIOT Act*, 72 Geo. Wash. L. Rev. 1145 (2004) (describing the history of the USA-PATRIOT Act's passage, which occurred less than two months after September 11th).

192. Kerr, *Fog*, *supra* note 127, at 814.

193. *See, e.g.*, *supra* notes 136-37 and accompanying text.

194. Kerr, *Constitutional Myths*, *supra* note 1, at 807.

required knowledge of quantum physics, Kerr's argument would have more resonance. In fact, Congress's electronic surveillance law is infinitely more complex than the technologies it seeks to regulate.

Expert testimony or an amicus brief can adequately explain the technology to judges in many cases. There is nothing to suggest that judges do not have the capacity to understand the Internet, e-mail, pen registers, and other technologies. Kerr is right that there are many times when judges are lazy and do not acquire a good understanding, but the same is true of legislators. Kerr does not offer a reason why the institutional structure of legislatures shields them from the tendency to be lazy, any more than the institutional structure of the judiciary shields the courts from laziness.

To illustrate his claim that new technologies are too complex for simple judicial minds to grasp, Kerr points to *United States v. Bach*.[195] The district court in that case, according to Kerr, misunderstood how "ISPs comply with court orders to produce records."[196] Is this an issue of high technology? Kerr wrote an amicus brief and the U.S. Court of Appeals for the Eighth Circuit agreed with him and reversed. This is an example of the courts getting it right and understanding the technology. Kerr himself helped supply the facts about the technology to the Eighth Circuit, and the judges decided the case correctly, according to Kerr. At most, this example demonstrates how a district court decided a case incorrectly and was then reversed by a court of appeals. This is hardly a demonstration of the failure of the judiciary to grasp the facts. By all accounts, this example demonstrates that the judicial process works. This is a success story. The judges got the correct information and decided the case correctly, according to Kerr.

Kerr then claims that this example is an anomaly: "[I]n most cases, courts will not possess an informed understanding of the technical facts they need to appreciate the technology they are attempting to regulate."[197] Why not? This is a bald assumption that Kerr's example does not support. The information necessary to understand the technology that Kerr describes is readily available. In fact, a search of Westlaw will reveal Kerr's own articles explaining this technology quite clearly and succinctly. All a judge has to do is pull up one of Kerr's articles and read about four pages to understand the technology. Why is this so complicated? Why is it beyond the time constraints and mental capacities of judges? The information about the technology is readily available and does not take an advanced degree in computer science to comprehend. It is dubious that the brilliant minds in Congress have more time to learn the workings of technology than judges concentrating on a specific case.

195. 310 F.3d 1063 (8th Cir. 2002) (holding that there is no Fourth Amendment requirement that an official be present when executing a warrant to retrieve e-mails from an ISP).

196. Kerr, *Constitutional Myths*, *supra* note 1, at 878.

197. *Id.* at 879.

Furthermore, merely shifting to a statutory regime will not eliminate Kerr's concern with judges misunderstanding technology. In fact, many judicial misunderstandings stem from courts trying to fit new technologies into old statutory regimes built around old technologies. The problem with the statutes is that, when they try to track existing technology too closely, they become too rule-like and lose the flexibility of a standard. Basic principles get lost or forgotten in the shuffle of technicalities. Discussions about whether certain new technologies fit into the labyrinthine framework of electronic surveillance law focus on elucidating confusing definitions or navigating complicated distinctions.

Principles should guide technology, not vice versa. Instead of focusing on statutory puzzles, the law should focus on the real issues at stake: Does a particular technology pose a threat to privacy? What are the dangers? How might they be mitigated or controlled?

Sadly, courts have also failed to address these important questions, instead turning on a crabbed conception of Fourth Amendment privacy that seems to have little connection to the issues raised above. As a result, the Fourth Amendment has been held inapplicable to many new technologies, creating the void that has been filled, rather poorly, by Congress. The answer to the problem of creating rules to regulate law enforcement and new technologies is not to call for judicial caution and leave it to legislatures to draft the primary law. Rather, the answer is simply to craft better rules.

B. *Difficult Questions for a Dualist Criminal Procedure Regime*

The legislative regime Kerr extols suffers from substantial problems both in process and substance. This Article has attempted to demonstrate why Kerr's argument for a legislative institutional advantage is in error. In doing so, I am not arguing that courts have an institutional advantage over legislatures. I remain highly skeptical of institutional competence arguments, which were a staple of the legal process jurisprudence of the 1950s and 1960s.[198] As Edward Rubin observes, the "central principle [of legal process jurisprudence] was that each governmental institution possesses a distinctive area of competence such that specific tasks can be assigned to that institution without reference to the substantive policies involved."[199] Elsewhere, I have contended that institutional competence arguments often assume that institutions have "an inherent and unchanging nature."[200] This is a dubious assumption. In the context of crafting rules to regulate law enforcement and new technologies, I am not convinced that either the legislatures or the courts have strong advantages over the other.

198. Solove, *The Darkest Domain*, *supra* note 113, at 1010-11.

199. Edward L. Rubin, *The New Legal Process, the Synthesis of Discourse, and the Microanalysis of Institutions*, 109 Harv. L. Rev. 1393, 1396 (1996).

200. Solove, *The Darkest Domain*, *supra* note 113, at 1011.

Despite the fact that I find Kerr's case in favor of legislatures to be wanting, his article is successful at dispelling myths that have long hung over criminal procedure. Kerr is quite right that criminal procedure is no longer a realm of judicial constitutional rules, but instead is increasingly becoming a regime of statutes.[201]

This development of a dualist regime of both judicial and legislative rules which sometimes overlap and interact requires significantly more attention. Thus far, the criminal procedure literature has ignored the fact that we are in a dualist regime, with both legislative and judicial rules. This raises many questions: How should courts and legislatures proceed? What should the proper response to the rise of legislative rules be for courts in particular, which used to have more of a monopoly on creating criminal procedure rules? In light of Congress's increasing foray into criminal procedure, what should the courts do?

When there is no legislative rule addressing an issue, courts should apply the Fourth Amendment without any deference or caution. This does not mean that the Fourth Amendment should always apply, but there is no justification for caution or restraint in applying it. The courts have taken too narrow a view of the Fourth Amendment with regard to many issues involving information, such as the third party doctrine.[202] Courts have restricted Fourth Amendment applicability based on a narrow conception of privacy, which has impeded courts in looking at the crucial question of whether a particular law enforcement practice creates a problem, and if so, how that problem ought to be addressed. In other words, the Fourth Amendment often gets caught up in an analytical game that loses sight of the problems. As a result, the Fourth Amendment does not protect against serious threats to privacy and many law enforcement abuses. A better approach toward applying the Fourth Amendment is definitely in order, and such an approach should not be discouraged in favor of the hope of legislative solutions.

A different scenario exists when courts must examine a case involving new technologies where a federal statute already exists to regulate law enforcement use of those technologies. These are cases where, for example, the Wiretap Act, Stored Communications Act, or Pen Register Act would apply. Courts could take a few possible approaches. First, in order to preserve the space upon which Congress has legislated, courts could hold that the Fourth Amendment does not apply. Such an approach should be rejected, as the federal legislation in many cases has not been sufficiently protective of privacy.

Second, courts could hold that the Fourth Amendment applies, and then determine whether Congress's legislation is adequate to satisfy Fourth Amendment requirements. This Article supports such an approach.

---

201. "[A] basic understanding of criminal procedure rules may someday require as much knowledge of the United States Code as the United States Reports." Kerr, *Constitutional Myths*, *supra* note 1, at 806.

202. Solove, *Digital Dossiers*, *supra* note 121, at 1133-38.

Although, in many cases, warrants supported by probable cause are the best form of protection,[203] warrants are a means to an end, not an end in themselves. Elsewhere, I identified three central principles embodied in the Fourth Amendment: minimization, particularization, and control.[204] Government investigations must be minimized to prevent sweeping dragnet searches. Investigations must be particularized to specific individuals suspected of criminal wrongdoing. And there must be meaningful oversight over law enforcement activities.

In any particular case in which the Fourth Amendment applies, courts should apply the Fourth Amendment as they normally would. But suppose that law enforcement officials were following a statute that establishes different procedures for conducting surveillance or searches than typical Fourth Amendment rules. Here, the courts should not hold the law enforcement activity invalid simply because it was not conducted pursuant to the regular Fourth Amendment rules the courts have established. These regular, judicial Fourth Amendment rules should be viewed as the default rules, not the only valid rules. Thus, courts should examine whether the statutory procedures followed by law enforcement in a given case satisfy the basic principles of the Fourth Amendment. If law enforcement officials follow a statutory provision that departs from regular Fourth Amendment procedures but nevertheless adequately addresses minimization, particularization, and control, then courts should conclude that the search was valid. Certainly, courts should not have a monopoly on crafting the rules, and this is where courts and legislatures can establish a useful dialogue.[205]

To illustrate this approach more concretely, suppose that Congress passes the Thermal Sensor Protection Act ("TSPA"). The TSPA provides a set of rules to regulate law enforcement use of a thermal sensor. The TSPA, however, also allows the use of a thermal sensor based on a court order that differs in its standards from the *Kyllo* requirements for a warrant supported by probable cause. Although the court order is not a warrant, it does have other built-in protections. Courts should not simply conclude that any procedures that differ from the traditional ones required in *Kyllo* are invalid under the Fourth Amendment. Instead, courts should examine whether the TSPA adequately addresses minimization, particularization, and control. If it does, then the surveillance should be upheld.

The Wiretap Act represents an example of this process. Under traditional Fourth Amendment doctrine, search warrants generally authorize a single search. A second search is sometimes justified if it "is a reasonable

203. *See* Solove, *supra* note 171, at 1299-1303.

204. Solove, Digital Person, *supra* note 22, at 211.

205. *See* Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 Mich. L. Rev. 904, 922 (2004) ("Dialogue and continued participation by both branches is likely to lead to better outcomes, for both majoritarian and counter-majoritarian reasons.").

continuation of the original search."[206] For electronic surveillance, these restrictive rules would not make much sense. Surveillance generally must be continuous and extend for a period of time in order to capture the necessary communications. The Wiretap Act authorizes a long period of surveillance, specifically a thirty-day order renewable for another thirty-day period.[207] This is much broader than the kind of search the Fourth Amendment typically permits. The Wiretap Act, however, has other protections to compensate for the departure from these minimization goals of the Fourth Amendment. It requires that courts place minimization procedures in surveillance orders, and it makes such orders harder to justify, with law enforcement officials having to explain why other investigative techniques would not be viable.[208] It limits the kind of officials who may obtain such an order to high-level officials.[209] As a result, it compensates for the thirty-day rule with other ways to achieve minimization. This provision came about because, just a year before its passage, the Court in *Berger* explained how Fourth Amendment principles were to be embodied in electronic surveillance law.[210]

In the *Berger* model, the Court played a leading role in the process. The Court laid down the basic principles and then let Congress work out the specifics. Courts should look to whether legislation comports with basic Fourth Amendment principles. Congress can fill in the gaps or be more precise where necessary, but this is a bold role for the courts, not a cautious one.

In short, courts should be very active in shaping new criminal procedure rules. To the extent that Kerr is urging courts to apply basic Fourth Amendment principles and be open to allowing legislatures to fill in the details, his advice is sound. But Kerr's article appears to suggest much more than that.

Kerr is right that we need to do a lot more thinking about our dualist system of criminal procedure. Scholars and many courts still operate under the assumption that the Fourth Amendment is the nearly exclusive occupier of the field. Now that we have a large body of statutory regulation, there are new questions about how we should modulate the relationship between the Fourth Amendment and the statutes.

Kerr's article has made a significant contribution. It is time for a focus on statutes. Unfortunately, the bulk of his article focuses on pushing the courts aside and suggesting a deferential approach based on faulty legal process arguments and an incorrect view of the effectiveness of the statutes.

206. United States v. Keszthelyi, 308 F.3d 557, 568 (6th Cir. 2002); *see also* United States v. Squillacote, 221 F.3d 542, 557-58 (4th Cir. 2000); United States v. Kaplan, 895 F.2d 618, 623 (9th Cir. 1990).

207. 18 U.S.C. § 2518(5) (2000).

208. 18 U.S.C. § 2518(1)(c).

209. 18 U.S.C. § 2518(11)(a)(i).

210. Berger v. New York, 388 U.S. 41 (1967).

Far from being cautious, courts need to take a larger role in the process to ensure that the statutes embody basic Fourth Amendment principles.