Michigan Law Review

Volume 102 | Issue 5

2004

Katz is Dead. Long Live *Katz*

Peter P. Swire
Moritz College of Law of the Ohio State University

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

 Part of the Criminal Procedure Commons, Fourth Amendment Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904 (2004).
Available at: https://repository.law.umich.edu/mlr/vol102/iss5/3

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

KATZ IS DEAD. LONG LIVE *KATZ.*

*Peter P. Swire**

Katz v. United States is the king of Supreme Court surveillance cases.[1] Written in 1967, it struck down the earlier regime of property rules, declaring that "the Fourth Amendment protects people, not places."[2] The concurrence by Justice Harlan announced the new regime — court-issued warrants are required where there is an infringement on a person's "reasonable expectation of privacy."[3] Together with the companion case *Berger v. New York*,[4] *Katz* has stood for a grand conception of the Fourth Amendment as a bulwark against wiretaps and other emerging forms of surveillance.

Professor Orin Kerr, in his excellent article, shows that this view of *Katz* fits badly with how courts now apply the Fourth Amendment to electronic surveillance and other new technology.[5] Upon reading his own obituary, Mark Twain famously observed that "reports of my death are greatly exaggerated."[6] This Essay shows that the demise of *Katz* has actually been understated. Professor Kerr has correctly shown how the property regime has persisted where it helped the government, such as cases that hold that many kinds of surveillance are not "searches" under the Fourth Amendment. This Essay adds the insight that the property regime has actually been abandoned in many other respects since 1967, in ways that have dramatically aided

---

* Professor of Law, Moritz College of Law of the Ohio State University. A.B. 1980, Princeton University; J.D. 1985, Yale Law School. — Ed. I became involved in the issues discussed in this article during my time as Chief Counselor for Privacy in the U.S. Office of Management and Budget and as Chair of a White House Working Group on how to update wiretap and electronic surveillance law for the Internet age. My thanks for research support from the Moritz College, and also for the graciousness of the George Washington University Law School for providing an office for me when I am in D.C. In that setting I have enjoyed numerous conversations with Orin Kerr. Thanks as well for helpful comments on this project from Akhil Amar, Joshua Dressler, Mike Seidman, Marc Spindelman, and Eugene Volokh.

1. Katz v. United States, 389 U.S. 347 (1967). *Katz*, for instance, has been called the "lodestar" in determining whether a government-initiated electronic surveillance is a search. Smith v. Maryland, 442 U.S. 735, 739 (1979).

2. *Katz*, 389 U.S. at 351.

3. *Id.* at 360 (Harlan, J., concurring).

4. Berger v. New York, 388 U.S. 41 (1967) (striking down New York's wiretap statute under the Fourth Amendment for failure to have sufficient safeguards).

5. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 799 (2004).

6. *See* THE NEW DICTIONARY OF CULTURAL LITERACY (3d ed. 2002), *available at* http://www.bartleby.com/59/6/reportsofmyd.html.

government surveillance. In particular, as discussed in Part I, the 1967 abolition of the "mere evidence" rule has given the government unprecedented access to diaries, private papers, and other information of individuals.

Examination of the case law and of new developments in telephone technology leads to a second insight. The shift to Voice over Internet Protocol phone calls means that the content of many telephone calls will likely be subject to routine recording in the near future. Because the Supreme Court has been so supportive of government access to stored records, *Katz* and *Berger* may soon be dead for their core facts, the content of phone calls.

If *Katz* is dead (or nearly so), what should be done? Professor Kerr appears to welcome the demise of *Katz*. He argues at length that Congress can do a better job than the courts at creating the law for high-tech surveillance. This Essay criticizes that view, showing reasons why Fourth Amendment doctrine should continue to play a role in governing electronic surveillance and other high-tech searches. At a minimum, the Court should announce basic principles for how surveillance can be conducted, with Congress then supplying the details.

The end of *Katz*, perhaps even on its own facts, invites us to consider what alternative approaches the courts might take in structuring a regime for high-tech surveillance by the government. This Essay sketches some of the substantive doctrines that courts might workably enforce in defining Fourth Amendment searches. It then explores in some detail the possibility that the courts can work collaboratively with the elected branches to ensure that there are reasonable procedures in place. The new regime would uphold the rule of law, with reasonable procedures specified in advance. This approach would give both the courts and the elected branches appropriate roles in important categories of searches, such as those involving emerging technologies, new types of surveillance, and complex record-keeping systems.

I. THE END OF THE PROPERTY REGIME AS SWORD, NOT SHIELD

A key achievement of Professor Kerr's article is to describe how the property approach to the Fourth Amendment has survived *Katz*: "[I]n most (though not all) cases, an expectation of privacy becomes 'reasonable' only when it is backed by a right to exclude borrowed from real property law."[7] He adds: "Although no one theory explains the entire body of Fourth Amendment doctrine, property law provides

7. Kerr, *supra* note 5, at 808.

a surprisingly accurate guide."[8] Despite the many citations to *Katz's* "reasonable expectation of privacy" test in the courts and in law reviews, there has been no case beyond wiretapping where application of the test has led to protection of privacy.[9] Put mildly, *Katz* has not been a good shield for privacy against intrusive new technologies.[10]

Professor Kerr's article thus helps us to see clearly what is happening — despite the comforting discussion of privacy expectations, the courts continue to apply a property-based approach to new technologies. This description, however, tells only half the story. The Supreme Court did in fact abandon the property-based approach in 1967 in ways that have continuing major effects, but it actually did so in the direction of reducing the privacy protection offered by prior law. In the same year as *Katz*, in *Warden v. Hayden*,[11] the Supreme Court abolished the "mere evidence" rule. That rule had previously set limits on the ability of a search warrant to authorize collection of documents and other "mere evidence" of a crime. By examining the shifts in the "mere evidence" rule, we can re-envision the 1967 abandonment of the property-based approach as a sword for greater entry into private spaces, and not the shield for protecting privacy that most have supposed.

The "mere evidence" rule was a matter of common sense under the property-based approach to the Fourth Amendment. A search warrant could lawfully issue for items where the property interest of the government was superior to that of the person holding the object. Notably, an individual could claim no legitimate property interest in the fruits of a crime, such as: stolen goods; its instrumentalities, such as the knife used in the crime; or in contraband, such as illegal narcotics. By contrast, a person's private papers were long understood to be outside the reach of a search warrant under the authority of the 1765

---

8. *Id.* at 813. In response to comments to earlier drafts, Professor Kerr now has a more modest claim about the extent to which the courts follow property rules. Professor Kerr argues that the property regime is the single best predictor of Fourth Amendment doctrine, but notes that "hyper-technical" property rules are not always followed. Although he briefly mentions *Warden v. Hayden*, Professor Kerr does not discuss the great extent to which the Fourth Amendment jurisprudence departs from the traditional property regime with respect to the "mere evidence" rule. *Id.* at 843.

9. A possible exception is the requirement of a warrant before using the thermal-imaging equipment at issue in *Kyllo v. United States*, 533 U.S. 27 (2001). Even in this instance, however, the majority decision by Justice Scalia heavily stresses the invasion of the quintessential property interest, the home, as a crucial reason for the constitutional protection. *See* Kerr, *supra* note 5, at 830-36 (discussing *Kyllo*).

10. For an examination of the limited nature of current protections against video surveillance and other "hyper-intrusive" searches, see Ric Simmons, *Can* Winston *Save Us from Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches*, 55 RUTGERS L. REV. 547, 556-60 (2003).

11. Warden v. Hayden, 387 U.S. 294 (1967).

case of *Entick v. Carrington*,[12] as interpreted by the Supreme Court in *Boyd v. United States*[13] and *Gouled v. United States*.[14]

Justice Brennan authored the opinion in *Hayden* that overturned the "mere evidence" rule. He stated: "The premise that property interests control the right of the Government to search and seize has been discredited."[15] Emphasizing that "the principal object of the Fourth Amendment is the protection of privacy rather than property,"[16] he foreshadowed by less than a year the statement in *Katz* that "the Fourth Amendment protects people, not places." Justice Brennan seems to have contemplated a symmetry in the change of doctrine. The "reasonable expectation of privacy" approach created a doctrine that would apply both in settings where government powers would expand (allowing seizure of the clothes found in *Hayden*) and would recede (prohibiting the wiretap in *Katz*). It is likely that Justice Brennan, writing for the liberal Warren Court, expected that the shift from the property approach to the privacy approach would result in an overall expansion of Fourth Amendment protections.

The opposite has occurred. On a doctrinal level, the Court has been far stingier in finding a "reasonable expectation of privacy" than Justice Brennan foresaw. The Court has swept aside limits on government access to documents that would have existed under the old property approach. The result of the new doctrine has been to open the door to a far greater number of document searches than was previously permitted. Aficionados of the Fourth Amendment are familiar with the key cases. The focus here will be on how the announced shift from the property to the privacy approach has affected government access to records held by third parties.

The narrow scope of the "reasonable expectation of privacy" test was established in *United States v. Miller*, which involved subpoenas for copies of checks written by the defendant.[17] The court of appeals struck down the subpoenas under the Fourth Amendment, citing the prohibition in *Boyd v. United States* against " 'compulsory production of a man's private papers to establish a criminal charge against him.' "[18] The Supreme Court reversed. Justice Powell for the majority found that the defendant had no reasonable expectation of privacy. Justice

12. Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765) (holding that a warrant cannot form the basis for the seizure of a person's private papers from the home).

13. Boyd v. United States, 116 U.S. 616 (1886) (ruling that compulsory production of a person's private papers cannot establish a criminal charge against the defendant).

14. Gouled v. United States, 255 U.S. 298 (1921) (reiterating *Boyd*).

15. *Hayden*, 387 U.S. at 304.

16. *Id.*

17. United States v. Miller, 425 U.S. 435 (1976).

18. *Id.* at 439.

Powell quoted *Katz* itself in saying " '[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.' "[19] The crucial doctrinal finding was that the "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[20] The subpoenas produced "only information voluntarily conveyed to the banks." Justice Brennan angrily dissented,[21] but *Miller* today stands for a broad proposition that individuals "voluntarily" reveal information when they give documents or data to third parties. Based on this individual "consent" to share data, the holders of data such as banks may pass on the data to the government without triggering Fourth Amendment requirements.[22]

The limits of the "reasonable expectation of privacy" test, and the government's broad access to stored records, were reaffirmed in *Smith v. Maryland*.[23] The case presented the question whether the installation and use of a pen register constitutes a "search" under the Fourth Amendment. "Pen registers" create a list of all of the numbers dialed from a telephone, just as "trap and trace" devices create a list of the numbers that call into a telephone.[24] The Court held that there was no "reasonable expectation of privacy" in the list of phone numbers dialed, because "petitioner voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record."[25] This emphasis on the government's access to

---

19. *Id.* at 442.

20. *Id.*

21. *Id.* at 447 (Brennan, J., dissenting). Justice Brennan did not believe there was true consent by the bank customer because "it is impossible to participate in the economic life of contemporary society without maintaining a bank account." *Id.* at 451 (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974) (Mosk, J.)). To permit the third party to share data with the government, without the Fourth Amendment applying, "opens the door to a vast and unlimited range of very real abuses of police power." *Id.* (Brennan, J., dissenting (quoting *Burrows*, 529 P.2d at 596).

22. One subject for further investigation would be to show a more explicit link between the abandonment of the "mere evidence" rule in *Warden v. Hayden* and the broad conception of "voluntary" disclosure in *Miller*. It seems logical to believe that once the government can get "mere evidence" from suspects themselves, it is easier to support the doctrine that the government can get any evidence held in the hands of third parties.

23. Smith v. Maryland, 442 U.S. 735 (1979).

24. For my views on a good legal regime for pen register and trap and trace orders, see Peter P. Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, Brookings Terrorism Project Website (October 3, 2001), *at* http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm [hereinafter Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*].

25. *Smith*, 442 U.S. at 745. The dissenting opinion by Justice Stewart would have found that the Fourth Amendment applied to the telephone numbers dialed from a residence, and said "I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called . . . and thus reveal the most intimate details of a person's life." *Id.* at 748 (Stewart, J., dissenting).

stored records has become increasingly important over time, as discussed further below.[26]

Although the Court found that the bank or the phone company owned the records in these cases, it made clear that defendants' ownership of records would not protect those records from the government. In *Couch v. United States*, the question was whether a taxpayer could invoke the Fifth Amendment privilege against compulsory self-incrimination to prevent the production of records in the possession of her accountant.[27] The *Couch* majority recognized the defendant's property interest in the papers, yet ruled that the papers had to be provided to the government.[28] Later Supreme Court cases similarly upheld the compelled production of documents where the government lacked any ownership interest.[29] Some justices wrote separately and at length to praise the cases protecting private papers from the eighteenth century (*Entick v. Carrington*), nineteenth century (*Boyd v. United States*), and twentieth century (*Gouled v. United States*). These justices condemned the unprecedented access of government to private papers, but their opinions were in concurrences and dissents.[30]

The Supreme Court also upheld the government's power to get records from third parties in the face of significant countervailing considerations. In *Fisher v. United States*, the government was able to compel production of papers held by a defendant's attorney, despite the attorney-client privilege.[31] Perhaps even more surprisingly, in 1978, *Zurcher v. Stanford Daily* permitted police to use a search warrant to take records held by a newspaper, despite First and Fourth Amendment objections to the search.[32] Justice Stevens in dissent

---

26. *See infra* Part II. Justice Stewart's dissent in *Smith v. Maryland* indicated the reasoning of the majority: "[T]he Court today says that [Fourth Amendment] safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes." 442 U.S. at 746 (Stewart, J., dissenting).

27. Couch v. United States, 409 U.S. 322 (1973). This Fifth Amendment issue had not arisen in *Warden v. Hayden*, which involved the question of whether production of a defendant's clothing was permitted under the Fourth Amendment's "mere evidence" rule.

28. The majority said: "Here petitioner does own the business records which the Government seeks to review . . . ." *Id.* at 327.

29. *E.g.*, Zurcher v. Stanford Daily, 436 U.S. 547 (1978) (documents held by student newspaper); Fisher v. United States, 425 U.S. 391 (1976) (documents held by an attorney).

30. *E.g.*, *Zurcher*, 436 U.S. at 577-78 n.1 (Stevens, J., dissenting); Fisher v. United States, 425 U.S. 391, 414 (1976) (Brennan, J., concurring in the judgment); *Id.* at 431 (Marshall, J., concurring in the judgment); Andresen v. Maryland, 427 U.S. 463, 489 (1975) (Brennan, J., dissenting);; California Bankers Ass'n v. Schultz, 416 U.S. 21, 94 (1974) (Marshall, J., dissenting); *Couch*, 409 U.S. at 339 (1973) (Douglas, J., dissenting).

31. Fisher v. United States, 425 U.S. 391 (1976).

32. Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

explained how the government search powers had expanded since the demise of the "mere evidence" rule:

> Just as the witnesses who participate in an investigation or a trial far outnumber the defendants, the persons who possess evidence that may help to identify an offender, or explain an aspect of a criminal transaction, far outnumber those who have custody of weapons or plunder. Countless law-abiding citizens — doctors, lawyers, merchants, customers, bystanders — may have documents in their possession that relate to an ongoing criminal investigation.[33]

Taken together, these cases show how Justice Brennan's vision in writing *Katz* and *Hayden* was turned on its head. The end of the property regime has become a sword for the government, not a shield of personal privacy. Professor Kerr's article documents how courts have clung to the property approach to assist the government, and have denied claims of a "reasonable expectation of privacy." The discussion here shows instead how courts have abandoned the property approach to assist the government and have permitted unprecedented access to documents and other stored information held by third parties.

II. ARE *KATZ* AND *BERGER* ALIVE ON THEIR OWN FACTS TODAY?

Under the case law and emerging facts, there is a surprisingly strong case for believing that *Katz* and *Berger* are no longer good law even for the contents of telephone calls. The message of *Miller* was that information voluntarily revealed to a third party, such as a bank, does not enjoy a "reasonable expectation of privacy." The message of *Smith v. Maryland*, as explained by Justice Stewart, was that Fourth Amendment safeguards "do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes."[34] The Stored Communications Act, first enacted in 1986 in the wake of *Smith*, permits the government to get access to the content of stored communications from a communications provider without a warrant.[35] Its complex rules allow access to the content of e-mail and other stored communications with less than probable cause.

What if the contents of ordinary telephone calls become stored as a matter of routine? This technological change would arguably, and

---

33. *Id.* at 579 (Stevens, J., dissenting).

34. Smith v. Maryland, 442 U.S. at 746 (Stewart, J., dissenting).

35. The Stored Communications Act, 18 U.S.C. § 2701, provides a complex variety of rules for government access to stored records, all of which are less strict than the traditional Fourth Amendment search warrant. For a detailed analysis of the Act, see Orin G. Kerr, *A User's Guide to the Stored Communications Act — And a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. (forthcoming 2004).

plausibly, transform the recording of the telephone call into a stored record subject to the Stored Communications Act. A search warrant would no longer be required.

This slide from content protected by the Fourth Amendment to stored records available under the Stored Communications Act has already begun. Voice mails were historically given the same protection as live telephone calls. The statutes implementing *Katz* and *Berger* had required a probable-cause warrant with the strict safeguards provided by Title III of the 1968 crime bill.[36] In 2001, however, Congress decided to treat voice mail as a stored record rather than the content of a telephone call in Section 209 of the USA PATRIOT Act.[37] The statutory language on its face would appear to permit access to the voice mail even if both parties were on the line having a conversation.[38]

The looming question is what will happen if and when ordinary phone calls themselves are routinely stored. This storage is likely to become far more common with the imminent growth of Voice over Internet Protocol ("VOIP") telephone calls.[39] VOIP uses the packet-switching network of the Internet to connect telephone calls rather than the traditional circuit-switching used by established phone systems.[40]

Use of VOIP is likely to result in a drastic increase in storage of the content of telephone calls for at least two reasons. First, the use of computers for making telephone calls makes it trivially easy for one party to store the contents of the conversation. This ease of storage makes a telephone call more like an e-mail, where users can foresee that the recipient may keep a copy of the communication or forward it to others. Doctrinally, the ease of storage would make it easier for

---

36. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197.

37. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, § 209.

38. Both parties might be on the line, for instance, if the voice mail machine had started recording before the recipient picked up the call or if the recipient simply turned on a voice mail recorder during a conversation. Section 209 extends to all "wire"-stored records, without consideration of whether there is a contemporaneous conversation between two parties.

39. For one overview of the emerging market for VOIP, see Peter Grant, *Ready for Prime Time: A New Internet-Based Phone Technology Has an Un-Catchy Acronym: VOIP*, WALL ST. J., Jan. 12, 2004, at R7. Growth projections for VOIP vary widely, but the *Wall Street Journal* reported in early 2004:

> By the end of this year, about 20% of the new phones being shipped to U.S. businesses will use VOIP technology, according to Yankee Group, a technology consulting firm based in Boston. By 2007 that figure should exceed 50%, and eventually almost all of the new phones shipped will use VOIP, Yankee Group predicts.

Id.

40. For one basic introduction to the technology, see Howstuffworks, "How Telephony Works," *at* http://computer.howstuffworks.com/ip-telephony.htm (last visited July 9, 2004).

future courts to say that a user has voluntarily consented to storage by a third party. That storage, in turn, makes it less likely that the courts will hold there is a reasonable expectation of privacy in the communication.

A second technical change with VOIP is the likelihood that there will be systematic "caching," or storage, of telephone communications at the network level. One existing product, for instance, is called "CacheEnforcer."[41] CacheEnforcer stores communications for a group of users, such as for a company or a network operated by a university. Network managers, not individual users, determine the caching procedures. The caching can help the network in various ways, including improving average network speed and assisting in network security. Doctrinally, the existence of pervasive caching of telephone communications could once again undermine the earlier holdings that there is a "reasonable expectation of privacy" in telephone communications.

The increasing storage of telephone calls is part of the much-broader expansion since 1967 of stored records in the hands of third parties. Although there are no Supreme Court cases on most of these categories of stored records, the *Miller* and *Smith* line of cases make it quite possible that the government can take all of these records without navigating Fourth Amendment protections. For instance, voice mail was rare in 1967, and e-mail practically unknown. Video cameras now exist in convenience stores, shopping malls, and a host of other locations, so that the telephone booth used in *Katz* itself could now easily be subject to recording. Financial transactions have shifted away from cash to credit card, debit card, and other recorded transactions.[42] Individuals now store their calendars, personal diaries, and family photographs online.[43] Even the movements of individuals are being increasingly recorded. With the rise of cellular telephones, and the regulatory requirement that such phones be readily located, the technology is in place to keep track of and store the movements of cell-phone users.[44]

---

41. The product website says: "Because the CacheEnforcer sits in front of your WAN [wide area network] or Internet link, all outbound traffic passes through it. By setting appropriate policies on the CacheEnforcer, network managers, not individual users, determine the appropriate caching policies for the entire network." Allot Communications Products, CacheEnforcer, *at* http://www.allot.com/html/products_cacheenforcer.shtm (last visited July 7, 2004).

42. On the shift from cash to recorded transactions, see Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461 (1999) [Hereinafter Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*].

43. *See* Deirdre K. Mulligan, *Reconstructing Privacy in a World of 'Business Records'*, 72 GEO. WASH. L. REV. (forthcoming 2004).

44. *See* David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1 (2003).

III. SHOULD THE COURTS PLAY NO ROLE IN HIGH-TECH SEARCHES?

Once telephone calls are routinely stored, *Katz* and *Berger* may be dead on their own facts. Under current doctrine, individuals have a "reasonable expectation of privacy" in the context of phone calls but not in stored records. The Supreme Court has offered no reason why stored records of telephone calls deserve constitutional protection while stored records of voice mail, e-mail, financial records, personal diaries, and locational information do not.

The factual shift to stored telephone calls puts enormous pressure on the "reasonable expectation of privacy" test. When applied to searches outside of the home, the only category that has met that test has been the content of telephone calls. With the spread of VOIP and computerized storage, many and perhaps most phone calls will be stored in the near future. In this future, current doctrine at most would offer constitutional protections only to the dwindling subset of phone calls that did not happen to be stored. As a matter of constitutional doctrine, the broad wording of the "reasonable expectation of privacy" test is a very bad match for "the fraction of telephone calls that are not stored." It is difficult to provide a principled basis for protecting only that fraction of telephone calls under the Fourth Amendment. Faced with these facts, courts very possibly would decide that there is no "reasonable expectation of privacy" outside of the home, and overrule *Katz* and *Berger* explicitly.

Although Professor Kerr does not specifically recommend overruling *Katz*, he does argue that Congress should be the primary protector of privacy against searches made by new technology. He states: "courts 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."[45] In choosing Congress over the courts, Professor Kerr argues that Congress can enact more flexible rules, can amend them more frequently, and can gain a fuller understanding of technology than the courts.[46] This Part of the Essay critiques Professor Kerr's minimalist view of the role of the courts in applying the Fourth Amendment to new technologies. At least four categories of argument support a continuing and substantial role for the courts: there are public choice problems with legislation in this field; the dynamic that has led to privacy legislation in the past is unlikely to continue in the future; constitutional pronouncements of the courts help create appropriate privacy legislation; and courts and

45. Kerr, *supra* note 5, at 803.

46. *Id.* at 857.

Congress working together can likely produce better results than Congress alone.

A. *The Public-Choice Advantages of Law Enforcement Over Privacy Proponents*

Professor Kerr is highly optimistic that Congress will reflect public preferences in its surveillance laws, rather than be shaped by rent-seeking or other public-choice problems.[47] I have written in greater detail elsewhere why there instead appears to be a "ratchet-up effect" — a systematic tendency toward permitting greater surveillance over time in the legislative process.[48] This tilt toward surveillance comes in part from expertise and institutional staffing in federal law-enforcement agencies. As these agencies face the detailed requirements of the Electronic Communications Privacy Act and similar statutes, they use their expertise much as any other regulated industry would in response to regulations that limit its preferred behavior.[49] The regulated industry of law enforcement has a concentrated interest in reducing regulation — pushing for fewer warrants, less onerous reporting requirements, and so on. The concentrated interest in reducing regulation contrasts with the dispersed interest the general public has in protecting privacy over the long term.

This classic public-choice problem of a concentrated industry defeating a dispersed public interest is exacerbated here by the existence of a mechanism law enforcement can use to achieve its deregulation goals. Whenever there is a dramatic public-safety emergency, the law-enforcement agencies rush to lock expanded powers into legislation before the emergency fades away.

The differing fate of surveillance legislation proposed before and after the attacks of September 11 illustrates this pattern. After a lengthy internal process, the Clinton administration proposed legislation in the summer of 2000 that contained both expanded powers for law enforcement and new privacy protections.[50] The House

---

47. *Id.* at 884 (stating that congressional action "generally reflects legitimate public preferences," however, not rent-seeking).

48. Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. (forthcoming 2004) [hereinafter Swire, *The System of Foreign Intelligence Surveillance Law*].

49. *See, e.g.*, MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965) (explaining advantages that concentrated interests, such as regulated industries, have over diffuse interests in the political process).

50. I chaired the White House Working Group that considered the proposal, which was introduced in 2000 as S. 3083. *See* Press Release, The White House, Assuring Security and Trust in Cyberspace (July 17, 2000), *at* www.peterswire.net (announcing legislation proposed by Chief of Staff John D. Podesta in remarks at the National Press Club). For the text of

Judiciary Committee considered the proposal in the fall of 2000, and overwhelmingly amended it in the direction of greater privacy protections.[51] The support for privacy legislation was not enough to advance the legislation further, however. Both law-enforcement advocates and privacy advocates had enough strength to freeze the status quo into place and block provisions that they opposed.

The freeze thawed immediately, however, after the attacks of September 11, 2001. The USA PATRIOT Act, drafted within a few days of the attacks, contained many of the pro-law-enforcement provisions that were contained in the 2000 Clinton proposal. It contained none of the pro-privacy proposals. Notably, it also contained a number of items from the law-enforcement "wish list" which had been omitted in the 2000 proposal.[52] A similar pattern occurred after the 1993 attack on the World Trade Center and the 1995 Oklahoma City bombing — quick introduction and then passage of legislation that expanded law-enforcement powers.[53] In light of these episodic, repeated expansions of law-enforcement powers, there is reason to believe that Congress will err over time on the side of surveillance and against privacy.

B. *The End of the Historical Patterns for Enacting Privacy Legislation*

Professor Kerr accurately notes that Congress has several times enacted legislation containing privacy provisions. He uses this fact to bolster his conclusion that "Congress has often taken the lead and . . . judicial decisions interpreting the Fourth Amendment generally have played a secondary role."[54] In fact, however, the role of the judiciary has been far more important than this quotation suggests. Supreme Court decisions have played a primary role in prompting and shaping privacy legislation to date. Congressional actions, when they have

---

Podesta's remarks, see Press Release, The White House, Remarks by the President's Chief of Staff John D. Podesta on Electronic Privacy to National Press Club (July 18, 2000), *at* www.peterswire.net.

51. Molly M. Peterson, *Panel Approves E-Mail, Phone Privacy Protections*, 32 NAT'L J. 3099 (2000).

52. For instance, Section 217 of the USA PATRIOT Act creates new authority for the government to receive e-mails and other electronic communications of "computer trespassers" without the need for a search warrant or other judicial process. A computer trespasser exception was considered but rejected for the 2000 legislation. *See* Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, *supra* note 24 (comparing 2000 and 2001 legislative proposals).

53. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994); Antiterrorism and Effective Death Penalty Act of 1996, Pub. L 104-132, 110 Stat. 1214.

54. Kerr, *supra* note 5, at 853.

occurred, have generally given far less protection than the Fourth Amendment norm of a probable cause warrant issued by a neutral magistrate. In addition, the way that the Court's decisions have influenced the legislature is unlikely to occur in the future, boding ill for privacy protections against new generations of high-technology searches.

The essential point is that Fourth Amendment cases generally offer a sharp yes/no choice between two positions. If the government action is a "search," then there are relatively strict rules. A neutral magistrate must decide whether "probable cause" has been shown. If the government action is not a "search," then the Fourth Amendment does not limit the government's access to the records.

The privacy legislation cited by Professor Kerr was enacted in response to Supreme Court decisions that government actions did not constitute a "search." Congress then stepped in to protect privacy interests, usually with statutory provisions less strict than a warrant requirement. For instance, the 1976 decision in *United States v. Miller* found no Fourth Amendment interest in bank records.[55] Congress responded in 1978 with the Right to Financial Privacy Act,[56] which was considerably less strict than getting a search warrant. An administrative summons is enough to get the records, without the need for a neutral magistrate.[57] Furthermore, the government need believe only that the records are "relevant to a legitimate law enforcement inquiry," rather than having to show probable cause.[58] In 1979, in *Smith v. Maryland*, the Supreme Court found no reasonable expectation of privacy in pen-register information.[59] Congress responded with the Electronic Communications Privacy Act of 1986.[60] That law sets forth a standard well below probable cause and calls for only a limited role for the magistrate. That magistrate "shall" issue the order whenever law enforcement "has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[61] A third example is the 1978 case of *Zurcher v. Stanford Daily*, where the Supreme Court found no need for a warrant in the search of a newspaper office for information about news sources.[62] The Privacy Protection Act of 1980

55. United States v. Miller, 425 U.S. 435 (1976).

56. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2000).

57. *Id.* § 3405.

58. *Id.*

59. Smith v. Maryland, 442 U.S. 735 (1979).

60. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

61. 18 U.S.C. § 3123(a) (2000).

62. Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

was enacted to fill that gap.[63] That Act is the only example on the list where the legislative privacy protections are at all comparable to the protections offered by a search warrant.

At least four mutually reinforcing reasons underscore the importance of judicial decisions to how these privacy protections were enacted. First, the Supreme Court decision made the issue more salient, focusing attention on a topic that otherwise would not climb to the top of the legislative agenda.[64] Second, the importance of the decision to the political process was greater because of what social scientists have called the "endowment effect"[65] or "status quo bias."[66] Described as "the most significant single finding from behavioral economics for legal analysis to date," the concept is that individuals experience a loss as more important than a gain of equal size.[67] Applied to the Fourth Amendment cases, the "status quo bias" helps us understand why the perceived "loss" of Fourth Amendment protections (in the eyes of those who previously believed the records were protected by a reasonable expectation of privacy) would be a spur to legislative action. Third, the opinions of the Supreme Court shaped the legislative debates. Vigorous dissents in each case articulated reasons why privacy protections should be considered important. The dissenting opinions would persuade some legislators that full Fourth Amendment protections were appropriate, but they could help persuade additional legislators that some sorts of legal protection, even at a lower level, should be enacted. Fourth, once the issue had moved high enough on the agenda to warrant a vote, there were persuasive public-policy arguments that some privacy protections were appropriate.[68] Otherwise, under the Supreme Court's holdings of no "search," the police would be able to see the private records without any legal process whatsoever.

The mutually reinforcing reasons for privacy legislation are unlikely to occur in the future. The triumph of the jurisprudence of *Miller* and *Smith* suggests little room for new decisions by the

63. 42 U.S.C. § 2000aa (2000).

64. For one good discussion of how issues rise and fall on a legislative agenda, see Michael E. Levine & Jennifer L. Forrence, *Regulatory Capture, Public Interest, and the Public Agenda: Toward a Synthesis*, 6 J.L. ECON. & ORG. 167, 191-94 (1990).

65. The term was coined by Richard Thaler. Richard Thaler, *Toward a Positive Theory of Consumer Choice*, 1 J. ECON. BEHAV. & ORG. 39, 44 (1980).

66. *See, e.g.*, William Samuelson & Richard Zeckhauser, *Status Quo Bias in Decision Making*, 1 J. RISK & UNCERTAINTY 7 (1988).

67. *See* Russell Korobkin, *The Endowment Effect and Legal Analysis*, 97 Nw. U. L. REV. 1227, 1229 (2003).

68. Levine & Forrence, *supra* note 64, at 191-93 (explaining why legislators are more likely to vote for their view of good public policy, rather than follow the wishes of special interest groups, once an issue has become salient).

Supreme Court that would prompt congressional action. Perhaps Congress would act if *Katz* were explicitly overruled or if the thermal imaging at issue in *Kyllo* were permitted.[69] Other than that, the factors that have historically led to limits on government access to records will not likely exist in the future. These past examples of privacy legislation do not support Professor Kerr's confidence that Congress will be aggressive in crafting privacy protections in the future.[70]

There is one other historical pattern for passage of privacy legislation, but that pattern does not fit Professor Kerr's thesis either. The Supreme Court has sometimes emphasized the importance of Fourth Amendment protections in an opinion and then invited Congress to fill in the legislative details. Professor Kerr documents how Congress was awaiting the outcome of *Berger* and *Katz* and used those opinions as the basis for the Title III protections of telephone wiretaps and bugging.[71] In 1972, the Court examined how the Fourth Amendment would apply to national-security cases, and the guidance in *United States v. United States District Court* (known as the *Keith* case) became the roadmap for the Foreign Intelligence Surveillance Act of 1978.[72]

In summary, Professor Kerr supports having Congress take *primary* responsibility for enacting new privacy protections as technology evolves. One criticism here is that privacy legislation to date has relied on a combination of factors, notably including a Supreme Court case finding no "search," that is unlikely to occur in the future. The second criticism is that the remaining privacy enactments have occurred in situations where the Supreme Court has acted in partnership with Congress — the Court announced constitutional principles while inviting the legislature to fill in the details. As argued below, this sort of partnership is an attractive model for applying the Fourth Amendment to new technologies. That

---

69. One might also see congressional action if the Supreme Court specifically held that medical records or private e-mails lacked Fourth Amendment protections. To date, neither of these cases has been presented to the Court.

70. There is one other possible combination of political forces that might lead to future legislation in the area. It is possible that changing technology will mean that law enforcement will see a need to gain specific authorities that were not previously as important. In that case, there is the possibility of a political compromise where law enforcement will gain those specific authorities while going along with privacy protections as part of a compromise. To understand the concept, consider how changing patterns of telephone use, including the possibility of buying several inexpensive cellular phones, has made it more important over time for law enforcement to have roving wiretap authority rather than the authority to tap a single phone line. Before the roving wiretap authority was authorized, it might have been tempting for law enforcement officials to agree to some new privacy protections if that were the price needed to get the roving wiretap authority.

71. Kerr, *supra* note 5, at 847.

72. *Id.* at 853 n.320 (describing the "extensive statutory guidance to Congress"); *see also* Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 48.

partnership, however, is contrary to Professor Kerr's approach. A review of the legislation to date shows little reason for confidence, despite the hopes of Professor Kerr, that Congress will step forward on its own to create limits on the government power to search records.

C. *How Retreat by the Court Would Likely Reduce Privacy Protections in the Political Process*

There is another way that reducing the courts' role in the Fourth Amendment would likely affect Congress's passage of privacy legislation. The title of Professor Kerr's article expresses the idea that the reasonable expectation of privacy has become a myth: *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*. Professor Kerr calls for discarding that myth, and instead having a Fourth Amendment "with constitutional rules governing most traditional cases and statutory rules governing most cases involving new technologies."[73] As discussed here, the Kerr approach would quite likely result in an impoverishment of the legislative debate about privacy and surveillance, and less effective deliberation on what safeguards are appropriate.

One chief flaw of the Congress-only approach is the ease with which proponents of surveillance can argue that the Constitution supports their position. A 2003 speech by Attorney General John Ashcroft shows how the Department of Justice claims that judicial acquiescence to searches shows approval for those searches:

> Since September 11, 2001, the Department of Justice has fought for, Congress has created, and the judiciary has upheld, legal tools that honor the Constitution.... It is a compliment to all who worked on the Patriot Act to say that it is not constitutionally innovative. The Act uses court-tested safeguards and time-honored ideas to aid the war against terrorism ....[74]

This passage wraps itself in the Constitution. It asserts that the PATRIOT Act contains "legal tools that honor the Constitution," "is not constitutionally innovative," and uses "court-tested safeguards." Each of these claims is subject to serious doubt.[75] Nonetheless, one can

---

73. Kerr, *supra* note 5, at 887.

74. Attorney General John Ashcroft, Prepared Remarks at the Federalist Society National Convention (Nov. 15, 2003), *at* http://www.politechbot.com/pipermail/politech/2003-November/000218.html.

75. For instance, prior to the PATRIOT Act federal courts had held that the Foreign Intelligence Surveillance Act ("FISA") required that "the primary purpose" of the surveillance must be foreign intelligence. *See, e.g.*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984). Because Section 218 of the PATRIOT Act, codified at 50 U.S.C. § 1804(a)(7), said that only "a significant purpose" of the legislation had to be for foreign intelligence, the PATRIOT Act raised the novel issue of whether secret FISA wiretaps could be used primarily for ordinary criminal investigations. *See generally* Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 48.

see how the cases discussed earlier in this Essay might support the claim that there are "court-tested safeguards" — the courts have indeed been presented with cases involving bank records, pen registers, and other sorts of records and have found there is no "search" under the Fourth Amendment. The safeguards under statutes such as the Right to Financial Privacy Act and the Stored Records Act are "court tested" in the sense that they have not been struck down as unconstitutional.

To sophisticated readers from the legal academy, there is a clear and large difference between a description of the Court's holdings — no "search" prohibited by the Fourth Amendment — and the claim that a particular surveillance technique is normatively desirable. In the political realm, however, the two statements can readily merge into the following: the courts have "tested" these safeguards, they are "not constitutionally innovative," and therefore the surveillance techniques are good.

The insight here is to recognize the moral and political authority of constitutional doctrine. The Constitution is imbued with what Madison in *The Federalist* called "that veneration which time bestows on everything."[76] The political criticisms of the PATRIOT Act, for instance, repeatedly state that it is unconstitutional. A Google search in late 2003 for "PATRIOT Act privacy unconstitutional" revealed 17,900 hits.[77] The way we Americans debate these issues is intimately intertwined with our view of the constitutional rules governing the government and the people. A great risk of the Congress-centered approach advocated by Professor Kerr is that the political and moral debate will be impoverished if the Court abandons the reasonable expectation of privacy test for high-technology surveillance.

Professor Kerr might respond, accurately, that he does not make the analytic mistake inherent in Attorney General Ashcroft's speech. Professor Kerr instead presents institutional arguments about why Congress acting alone will create better rules. He might argue, in addition, that the political debates might actually improve once everyone recognizes that Congress will have to take responsibility for the issues and the courts will not provide a constitutional safety net.

In response, although it is possible that Professor Kerr's estimate of the political debate will prove true, there is a great risk that it will not and that we will end up with considerably fewer protections

76. THE FEDERALIST NO. 49, at 314 (James Madison) (Clinton Rossiter ed., 1961).

77. The search was conducted on December 22, 2003 at www.google.com. Review of a sample of those sites shows repeated arguments that surveillance provisions in the PATRIOT Act are both bad policy and contrary to the Constitution. Another Google search, on the same date, of "PATRIOT Act unconstitutional privacy reasonable expectation" turned up 1,590 hits. Many of the sites based their arguments about unconstitutionality on the "reasonable expectation of privacy" test.

against intrusive government surveillance. For one thing, the discussion above[78] of statutes such as the Right to Financial Privacy Act and the Electronic Communications Privacy Act showed that the protections enacted by Congress were far less protective than a Fourth Amendment warrant requirement would have been for the same surveillance. The only statute that came up to the Fourth Amendment level of protection was the Privacy Protection Act, where the equivalent of constitutionally required warrants was created for the narrow category of searches of publishers for material protected by the First Amendment. In short, when it has acted, Congress has enacted privacy protections considerably weaker than those imposed by the Fourth Amendment. In addition, as argued in the previous section, the historical pattern for Congress legislating — reacting to a controversial Supreme Court decision finding no "search" — is less likely to occur in the future.

Professor Eugene Volokh has made an intriguing additional argument about why Congress may be reluctant to enact privacy legislation in areas where the courts have found that the government is acting constitutionally. Professor Volokh argues that Congress may be acting in a "rationally ignorant" way when it defers to the constitutional holdings of the courts:

> The proper scope of police searches, for instance, is a complex issue. Most people lack well-developed, comprehensive philosophies on the subject that would give them clear answers to most police search questions. So instead of thinking deeply through the matter themselves, they may choose to defer to the Court's expert judgment, if they think that the Justices are usually (even if not always) right on such questions. Because people lack the time and ability to figure out what's right or wrong entirely on their own, they use legal rules as one input into their judgments.[79]

A shift from the reasonable expectations of privacy test to the Kerr approach, in short, risks damage to the political guarantees against excessive surveillance. The shift could impoverish the rhetoric about the risks of new surveillance, undercut existing arguments that provisions are unconstitutional, and bolster the analytically questionable argument that a statute is good just because the courts have decided not to strike it down.

---

78. See *supra* text accompanying notes 56-60.

79. Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026, 1080 (2003).

D. *The Potential for Privacy Protection by Both Congress and the Courts*

Professor Kerr comes down strongly on the side of Congressional rather than judicial protection of privacy rights: "legislatures often are better situated than courts to protect privacy in new technologies."[80] While stressing that the courts should be "cautious" in holding that the Fourth Amendment applies to new technologies,[81] Professor Kerr at no time indicates a single new technology that merits a finding of a "reasonable expectation of privacy" or the need for a Fourth Amendment search warrant. My own position, by contrast, is that courts properly can and should play a significant role in defining how the Fourth Amendment applies to new technologies. The history of privacy legislation reveals that judicial holdings and language have shaped subsequent legislation in intricate and helpful ways.

Dialogue and continued participation by both branches is likely to lead to better outcomes, for both majoritarian and counter-majoritarian reasons. As a matter of majoritarian politics, the analysis here shows public-choice reasons for believing that legislation will tilt over time toward greater surveillance than the public would wish; the patterns of legislation suggest that episodic crises will lead to authorization for expanded surveillance. At the same time, the main stimuli for privacy legislation against government surveillance are less likely to exist in the future.[82]

The counter-majoritarian role of the courts also counsels that courts continue to involve themselves in high-technology surveillance.[83] The Bill of Rights exists in large measure to provide a check on the passions of the majority as it acts through the legislative branch. Political opponents of the government, civil rights groups, non-citizens, and other minority groups have historically been the targets of intrusive surveillance.[84] It is emphatically the role of the

---

80. Kerr, *supra* note 5, at 886-87.

81. *Id.* at 806.

82. I have written elsewhere about how the gap between long-term and short-term preferences may lead to an undervaluing of the public's actual preferences about privacy. There appears to be a large preference in the long run for privacy protection, in order to avoid creating a "Big Brother" society. In the short-term, however, individuals often seem willing to give up privacy protection in favor of security, efficiency, and other goods. *See* Peter P. Swire, *Efficient Confidentiality for Privacy, Security, and Confidential Business Information*, BROOKINGS-WHARTON PAPERS ON FINANCIAL SERVICES (2003).

83. The counter-majoritarian role for the courts is most prominently articulated in JOHN HART ELY, DEMOCRACY AND DISTRUST (1980); *see also* Michael J. Klarman, *Majoritarian Judicial Review: The Entrenchment Problem*, 85 GEO. L.J. 491 (1997) (defending the counter-majoritarian approach).

84. For this history, see Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 48. On the ways that intrusive surveillance has targeted minority groups and

judiciary to enforce the Fourth Amendment and other constitutional protections where there is such good reason to suspect majoritarian abuses.

IV. LONG LIVE *KATZ* — NEXT STEPS FOR THE COURTS

The death of *Katz* would create a very odd constitutional regime where the most common and extensive searches — those using effective new technologies — are placed outside of the Fourth Amendment. The development of VOIP creates a *reductio ad absurdum*, in which the only expectations of privacy that are constitutionally "reasonable" are the dwindling few telephone calls that do not happen to be stored anywhere. In the face of this absurdity, the Supreme Court should find a new path that preserves an effective role for the courts while also adapting to changing technology. This Essay is not committed to explaining precisely what doctrine the courts should then adopt. Instead, the Essay sketches both substantive and procedural doctrines that could create a new life for *Katz*. The proposals here would help create a constitutional regime with a manageable judicial role likely to meet both the public-safety and privacy goals of the Fourth Amendment.

A. *More Substance for the "Reasonable Expectation of Privacy" Test*

Courts could maintain a role for the Fourth Amendment and rescue the *Katz* and *Berger* holdings by giving greater substance to the "reasonable expectation of privacy" test. Put simply, the courts could engage in a more substantive review of expectations of privacy in specific factual settings, and find that more categories of government action violate that test. This approach would recognize how the doctrines of consent and stored records now mean that there is rarely a high-tech "search" for Fourth Amendment purposes.

Scholars such as Patricia Bellia and Deirdre Mulligan are now exploring doctrinal approaches for treating some communications as "searches" under the Fourth Amendment.[85] One example would be to consider it a "search" when a third party, acting as a virtual bailor of data, reveals that data to the government. An Internet Service Provider ("ISP"), for instance, may promise to hold a user's e-mails on a secure server. The ISP would have reason to access those e-mails only in extraordinary situations similar to when a phone company listens to a call. In both instances, the company appropriately accesses

---

otherwise been a tool of discrimination, see Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, *supra* note 42.

85. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 72 (forthcoming 2004); Mulligan, *supra* note 43.

the communications for purposes of maintaining the system, but otherwise does not learn the content of communications. These bailor situations can be distinguished from a bank processing a payment, where bank employees routinely see the content of the communications (payor, payee, amount of payment, etc.) as an ordinary part of the transaction.

Privileged communications, such as with a medical provider or member of the clergy, could comprise another distinguishable category. Where a jurisdiction recognizes a testimonial privilege, there is a strong argument that the individual has not "consented" to turn the information over to the government simply because the information is in the hands of a third party. A database of electronic medical records or e-mails to a member of the clergy would be strong candidates for protection under a substantively enhanced "reasonable expectation of privacy" test.

A likely objection from Professor Kerr would be that courts lack the necessary expertise to understand the technology and create good categories for stricter Fourth Amendment protections. But there are standard ways that courts have managed to address issues involving complex technology in other contexts. Notably, courts in products liability and other cases have learned to use expert testimony about the technology. Defendants seeking to show a "reasonable expectation of privacy" in a factual setting might introduce this kind of expert testimony. Similarly, courts might draw on polling data to learn about the public's expectations of privacy. In discerning those expectations, courts could also review legislative enactments, which may be persuasive evidence of greater public concern about certain categories of surveillance.

In this brief Essay, there is no opportunity to flesh out all the details of a regime with a stricter substantive test for "reasonable expectation of privacy." Academics such as Professors Mulligan and Bellia are currently examining these doctrinal categories. More broadly, perhaps other experts in evidence and criminal procedure can pursue the best mechanisms for creating and administering these substantive categories.

B. *A Procedural Test for the "Reasonableness" of High-Tech Surveillance*

Less explored to date is a complementary way for courts not to abdicate all responsibility for the rules of high-technology surveillance. This approach would require judicial review of the reasonableness of the process used to create surveillance rules. This sort of test for reasonable process had been proposed previously, but apparently not for the subset of searches that involve emerging technologies and complex record-keeping systems. I offer arguments here why the

requirement of a reasonable process is especially appropriate for those categories of searches.

The proposal here builds on at least five different sources: Professor Amsterdam's call for "reasonable particularity" in drafting rules for searches under the Fourth Amendment; Professor Simon's explanation for why procedural rather than substantive rationality is more appropriate in complex technological settings; Professor Amar's emphasis on the general "reasonableness" requirement under the Fourth Amendment; the jurisprudence under Article 8 of the European Convention of Human Rights, where the European Court of Human Rights has required legislatures to set forth in advance the rules for surveillance; and the U.S. Supreme Court's own successes in *Katz*, *Berger*, and *Keith* in prompting Congress to craft detailed rules governing surveillance.

First, the procedural approach builds on the proposal of Professor Anthony Amsterdam in his classic article, *Perspectives on the Fourth Amendment*.[86] Professor Amsterdam emphasized the need to cabin the discretion of law-enforcement officials in conducting surveillance. He proposed a three-part rule:

> (1) Unless a search or seizure is conducted pursuant to and in conformity with either legislation or police departmental rules and regulations, it is an unreasonable search and seizure prohibited by the fourth amendment. (2) The legislation or police-made rules must be reasonably particular in setting forth the nature of the searches and seizures and the circumstances under which they should be made. (3) The legislation or rules must, of course, be conformable with all additional requirements imposed by the fourth amendment upon searches and seizures of the sorts that they authorize.[87]

The principal argument supporting this approach was the importance of cabining discretion and protecting against arbitrary searches and seizures.[88] Similar proposals have been made by other eminent authorities.[89]

The case for court review of reasonable procedures is significantly stronger if limited to the context of emerging technologies.[90] One

---

86. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).

87. *Id.* at 416-17.

88. *Id.* at 419.

89. *E.g.*, KENNETH CULP DAVIS, DISCRETIONARY JUSTICE: A PRELIMINARY INQUIRY 52-161 (1969); John Kaplan, *The Limits of the Exclusionary Rule*, 26 STAN. L. REV. 1027, 1050-55 (1974); Carl McGowan, *Rule-Making and the Police*, 70 MICH. L. REV. 659 (1972).

90. I do not take a position here about the precise effect of a failure by law enforcement to write surveillance rules in advance. Professor Amsterdam's proposal was apparently to find the search unreasonable per se in the absence of prior written rules. An alternative would be for courts to give substantially greater deference where prior rules exist, but not to find the lack of rules necessarily fatal to a search.

reason is that the procedural review can occur for a relatively contained subset of Fourth Amendment searches. Professor Amsterdam's proposal sought to apply more broadly, including for ordinary stops on the street and other traditional searches. It is possible, however, that judges would be hesitant to insist on formalized rulemaking for so many different types of searches. Instead of insisting on written rules for all searches, a better approach might be to allow judges to reach their own judgments, based on their own experience, about the constitutionality of traditional searches. Judges would use the procedural test in more limited settings, for emerging technologies, new types of surveillance, and complex record-keeping systems. The requirement of prior written rules would be less burdensome when applied to this subset of searches. Investigative guidelines might be written, for instance, for a relatively contained set of categories such as location information from cell phones, pen-register orders, the contents of e-mail or telephone conversations, and so on. The effort of writing these rules would be limited to the complex, technical settings where judges are less likely to have personal experience about the reasonableness of police conduct.

A second source, the writings of Nobel laureate Herbert Simon, underscores the likelihood that procedural review is especially appropriate in complex, technical settings. In his book *The Sciences of the Artificial*, Professor Simon studied complexity based on his research into economics, cognitive psychology, computer science, and related fields.[91] A central point of his research is that the nature of rationality changes in the face of additional complexity. For simpler problems, a decisionmaker seeks "substantive rationality." Roughly speaking, that means getting the correct answer. In Fourth Amendment terms, for instance, that would mean the courts would reach a judgment in a particular case about whether the Fourth Amendment would apply. As problems become more complex and difficult to understand, however, Simon stresses that one shifts to "procedural rationality." As complexity rises, the best one can hope for is to design a good process. We become willing to accept the judgment of appropriate decisionmakers acting in their areas of expertise, subject to review where needed.

In Fourth Amendment terms, the complex and shifting problems raised by new technologies call out for a "procedural rationality" approach. A manageable role for the courts is to police the system to ensure that reasonable rules are drafted for the new technologies. The absence of any legal rule is a red flag suggesting that no responsible officials have yet defined where surveillance is permitted or not.

---

91. HERBERT A. SIMON, THE SCIENCES OF THE ARTIFICIAL (1981).

A third source is Professor Akhil Amar's work, drawing on earlier work by Telford Taylor and others, on the nature of "reasonableness" under the Fourth Amendment.[92] Professor Amar has emphasized that the text of the Fourth Amendment has distinct clauses. The Warrant Clause, requiring a probable-cause warrant signed by a neutral magistrate, was the focus of most of the attention when the Supreme Court issued *Katz* and crafted other doctrines that limited unlawful searches. Professor Amar contrasts this with the opening language of the Fourth Amendment, which states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[93] In order to enforce this general reasonableness requirement, Professor Amar writes: "[T]he less specifically the legislature has considered and authorized the practice in question, the less willing judges and juries should be to uphold the practice."[94]

There may be a special reason to use this reasonableness approach in areas involving emerging technologies and complex record-holding systems. Statutory and regulatory privacy schemes already tend to be more nuanced. The medical-privacy rules in the United States, for instance, have complex provisions for medical research,[95] public health,[96] and especially for disclosure to law-enforcement officials.[97] Disclosures in some instances require much less of a showing than probable cause, such as for medical research that is done under procedural safeguards. Disclosure of a medical file to the police, by contrast, requires a greater showing of need, with even stricter rules applying to psychotherapy notes.[98] The degree of complexity in medical-privacy rules, which is mirrored in regimes such as those for financial privacy[99] and electronic communications,[100] suggests the

92. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994). Professor Amar dedicates this article to the memory of Telford Taylor, and the article builds generally on TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION (1969).

93. The amendment in full provides:

> 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.

U.S. CONST. amend IV.

94. Amar, *supra* note 92, at 816.

95. 45 C.F.R. § 164.512(i) (2003).

96. *Id.* § 164.512(b).

97. *Id.* § 164.512(f), (i).

98. *Id.* § 164.512(e). The provision for psychotherapy notes is at *id.* § 164.508(a)(2).

99. Financial-privacy rules are contained in Title V of the Gramm-Leach-Bliley Act of 1999. 15 U.S.C. §§ 6801-6827 (2000). The complex exceptions, which permit greater disclosure, are contained in Section 502(e) of the Act. *Id.* § 6802.

bluntness of a one-size-fits-all warrant requirement.[101] The medical-privacy rules were issued after the Department of Health and Human Services received over 50,000 comments on an enormous range of issues,[102] and it is unlikely that the one-size-fits-all warrant would be appropriate for that whole range of situations.

A fourth source, less familiar to most American scholars, is the body of law developed under Article 8 of the European Convention on Human Rights.[103] The European Court of Human Rights has used Article 8 on a number of occasions to strike down surveillance practices of the member states. Because the wiretapping and other surveillance practices in the member states and the United States are so similar, it is illuminating to see how the Court has interpreted Article 8 to set limits on high-technology searches while also permitting the elected branches to create the actual rules governing such surveillance.

The text of Article 8 echoes the Fourth Amendment. Paragraph One says: "Everyone has the right to respect for his private and family life, his home and his correspondence." This language echoes the "right of the people to be secure in their persons, houses, papers, and effects." Paragraph Two says: "There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of" various public purposes such as national security and the prevention of crime.[104] This language echoes the ban on "unreasonable searches and seizures," although with differences noted below.

Jurisprudence under Article 8 has emphasized that surveillance must be done "in accordance with the law." In 1979, the European Court of Human Rights interpreted this term, saying:

---

100. 18 U.S.C. §§ 2701-2711 (2000).

101. For a contrasting view, arguing for warrants across a very wide range of circumstances, *see* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. (forthcoming 2004).

102. For information on the development of the medical-privacy rule, see http://www.hhs.gov/ocr/hipaa.

103. For a discussion of the structure of the European Court of Human Rights, see Laurence R. Helfer & Anne-Marie Slaughter, *Toward a Theory of Effective Supranational Adjudication*, 107 YALE L.J. 273, 293-97 (1997). For discussions of the role of Article 8 in governing surveillance by the member states, see DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 691-713 (2003). For a discussion of Article 8 within the broader context of international human rights law, see George E. Edwards, *International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy*, 26 YALE J. INT'L. L. 323, 396-98 (2001).

104. The full list of public purposes that may justify interference with Article 8 rights are: "national security, public safety[,] the economic well-being of the country . . . the prevention of disorder or crime . . . the protection of health or morals, [and] . . . the protection of the rights and freedoms of others."

> First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct.[105]

The requirement of sufficient precision is most relevant to the idea that the U.S. Supreme Court should adopt a procedural view of the "reasonableness" of surveillance actions. The 2001 case of *P.G. & J.H. v. United Kingdom* gives a sense of the European Court's approach.[106] In that case, individuals challenged the government's ability to get billing records on telephone calls.[107] The Court upheld this government action, saying that detailed statutes governing billing records meant that the search was "in accordance with the law." On the other hand, the Court acted to strike down government action in response to the individuals' complaint: "that their voices were recorded secretly when they were being charged in the police station and while they were being held in their cells."[108] The Court stated that "the police knew that the applicants had refused to provide voice samples voluntarily and sought to trick them into speaking in an underhand procedure which was wholly unregulated, arbitrary and attended by bad faith."[109] Due in large part to this lack of established procedures, the Court found that the covert taping violated Article 8. In order to carry out such searches, the United Kingdom would need to create a legal structure to guard against the possibility of abuse.[110]

The well-developed jurisprudence under Article 8 can inform U.S. law for a number of reasons. For one thing, the nature of surveillance, searches, and technology is much the same in the United States and the member states of the European Convention on Human Rights. Telephone calls, e-mails, and credit card records are quite similar. For another, the tension between liberty and public safety is much the same, with member states such as Britain and Spain having faced

---

105. Sunday Times v. United Kingdom, 2 Eur. H.R. Rep. 245, 271 para. 49 (1979). In addition, legal rules would need to comply with the Article 8 language that the search be "necessary in a democratic society." This has been interpreted to mean that the surveillance be "proportionate to the legitimate aim pursued." Solove & Rotenberg, *supra* note 103, at 694. This proportionality test is similar to the requirement in U.S. law that searches be "reasonable."

106. 9 Eur. Ct. H. R. 197 (2001).

107. This information could be obtained in the United States under the Stored Communications Act, 18 U.S.C. § 2701 (2000), or through pen-register or trap-and-trace orders, 18 U.S.C. § 3122 (2000).

108. *P.G. & G.H.*, 9 Eur. Ct. H. R. at 215-16.

109. *Id.* at 216.

110. Similarly, the Court in an earlier case had struck down wiretapping by the British government in the absence of clear statutory procedures for monitoring the phone calls of private citizens. Malone v. United Kingdom, 7 Eur. H.R. Rep. 14 (1984).

domestic terrorism for a considerable period. In light of these similarities, the jurisprudence under Article 8 shows us an apparently successful role for the courts in requiring the legislative and executive branches to announce and implement rules to govern surveillance activities. In *Lawrence v. Texas*, the majority of the United States Supreme Court found it useful to cite to the jurisprudence of the European Court of Human Rights.[111] Put rhetorically, why should U.S. constitutional protections against government intrusion be less than those that exist in the European democracies?

A fifth source supporting the use of the procedural approach advocated here, is the catalog of instances where the Supreme Court worked collaboratively with Congress to create surveillance rules. As discussed above, the Court in *Katz* and *Berger* provided a template for Congress to write the detailed rules in Title III. Similarly, the Court in *Keith* supplied terms such as "foreign intelligence" and "agent of a foreign power" that became the heart of the Foreign Intelligence Surveillance Act of 1978. In both instances, decisions of the Supreme Court invited Congress to write detailed statutes concerning surveillance. This sort of collaboration of the two branches likely draws on the strengths of each — the role of the Court in seeing areas where there are constitutional problems and the role of Congress in writing prospective rules that take account of the intricacies of a substantive area of law.[112]

Based on these five sources, there is a strong case that the courts should play a role in insisting on the rule of law for searches that involve emerging or intrusive technologies and complex record-

111. Lawrence v. Texas, 539 U.S. 558, 573 (2003). The Supreme Court relied on the European Court of Human Rights to show the extent to which a position was reasonable or generally accepted. The Supreme Court said: "Authoritative in all countries that are members of the Council of Europe (21 nations then, 45 nations now), the [European] decision is at odds with the premise in *Bowers* that the claim put forward was insubstantial in our Western civilization." *Id.* This finding of substantial support in Europe for a position would be analogous to the Supreme Court determining whether a set of surveillance procedures is reasonable.

112. I will not attempt here to make a full defense of why I find Title III and FISA to have been generally successful statutes. As a brief defense, however, I note that both statutes were the result of extensive deliberation before passage. Both statutes kept their essential shape for a long time, with the basic outline of Title III continuing today for wiretaps and the basic outline of FISA staying roughly the same until the USA PATRIOT Act in 2001. In addition, both statutes offered significant privacy protections while also enabling surveillance to proceed. The level of protection contrasts sharply, for instance, with the level of protection provided by Congress for pen-register and trap-and-trace orders after the Supreme Court found no constitutional protection in *Smith v. Maryland*. Instead of the relatively strict showing of probable cause, a pen-register order issues where the evidence "is relevant to an ongoing criminal proceeding." 18 U.S.C. § 3122 (2000). In addition, the pen-register statute says that the magistrate shall issue the order upon a certification by law enforcement that the standard has been met, rather than making an independent evaluation. *See* Swire, *Administration Proposal Hits the Right Issues But Goes Too Far*, *supra* note 24 (analyzing pen-register rules).

keeping systems. The mere fact that a person told confidential information to a doctor, wrote an email to a person, or placed a personal diary on a secure server does not mean the person has, in the words of *Katz*, "knowingly exposed" that information "to the world." Like the European Court of Human Rights under Article 8, U.S. courts have much experience with reviewing the actions of the executive branch[113] and the legislature[114] to ensure a minimum level of reasonableness.

CONCLUSION

The King is dead! Long live the King! If *Katz* is the king of Fourth Amendment surveillance cases, then that king is dead. The "reasonable expectation of privacy" test has not been used to find such expectations beyond the original facts of *Katz* and *Berger*. Those cases themselves are subject to challenge in light of subsequent case law and the coming of stored telephone calls. If the courts are to play any role in applying the Fourth Amendment to emerging technologies, then we need a new king, a new doctrinal explanation of surveillance and the Fourth Amendment.

To shift metaphors from kings to cats, *Katz* has already had two lives. The first was as the protector of privacy envisioned by Justice Brennan and celebrated in the "reasonable expectation of privacy" test. The second has been as an invader of privacy. Its abandonment of the property regime was linked with the abandonment of the "mere evidence" rule, allowing access to innumerable private papers that had been inviolate under *Boyd v. United States*. Other language in *Katz* opened the door to the later holdings that individuals had "consented" to releases of information in the hands of third parties.[115]

My attempt here has been to suggest a third life for *Katz*, or at least for some court role in applying the Fourth Amendment to the many intrusive searches that employ new technologies or seek private information held by third parties. One new role for the courts would be what many had thought was the old role — a searching substantive inquiry into whether a search violates a person's "reasonable expectation of privacy." There is room within the Supreme Court

113. For instance, consider the role of courts in reviewing notice and comment rulemaking under the Administrative Procedure Act, 5 U.S.C. § 553 (2000).

114. For instance, courts have applied intermediate scrutiny to commercial speech under the doctrine of Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557 (1980). That test inquires whether "the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest." *Id.* at 566.

115. *See supra* text accompanying note 19 (discussing language in *Katz* to the effect that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection").

precedent to find a Fourth Amendment interest in e-mails and other information held in trust by third parties.

Another new role for the courts, and one that deserves far more attention than it has received to date, is procedural scrutiny requiring the elected branches to create a reasonable regime for surveillance. Such procedural review matches well with each institution's strengths concerning high technology searches. The European Court of Human Rights has played this role in Europe with good effect. In addition, collaborative efforts by the courts and the Congress resulted in the relatively stable and successful regimes under Title III and the Foreign Intelligence Surveillance Act, indicating that continued collaboration between the judiciary and legislature could be a viable option for the United States.

We live in a democracy. As such, it may seem odd to ask for a new way for the elected institutions to be overruled by the courts. Yet that is, of course, a chief purpose of the Fourth Amendment and the Bill of Rights more generally. The courts should play a role in setting rules for the unprecedented surveillance enabled by new technologies. Professor Kerr has helped us see more clearly what the courts have in fact been doing to date. He errs, I believe, in failing to put forward the rightful role that courts should play in controlling government searches in the future.