Hastings Law Journal

Volume 54 | Issue 4 Article 7

1-2003

State Wiretaps and Electronic Surveillance after September 11

Charles H. Kennedy

Peter P. Swire

State Wiretaps and Electronic Surveillance After September 11

by
CHARLES H. KENNEDY & PETER P. SWIRE*

For this symposium on Enforcing Privacy Rights, this Article turns its attention to an area of longstanding, large, and growing significance—the use of wiretaps and other electronic surveillance at the state level. The longstanding importance of wiretap law to enforcing privacy rights is underscored by the 1928 case of *Olmstead v. United States*.[1] The Supreme Court in *Olmstead* permitted a police wiretap without a search warrant of telephone calls from a home.[2] The case is best remembered, however, for the dissent by Justice Brandeis, who declared: "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping."[3] Justice Brandeis famously continued that "[t]he makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[4]

As discussed in more detail below, the Supreme Court in the 1960s eventually shifted to the position of Justice Brandeis. It held that wiretaps by both federal and state officials are subject to constitutional scrutiny where there is a reasonable expectation of privacy.[5] Congress then enacted wiretap and electronic surveillance

---

* Charles H. Kennedy is a partner with Morrison & Foerster, LLP. Peter P. Swire is Professor of Law at the Moritz College of Law of the Ohio State University and a consultant to Morrison & Foerster, LLP. For the underlying survey of the state wiretap and electronic surveillance laws, the authors are grateful for assistance by attorneys and researchers at Morrison & Foerster including Laurence Bolton, Jennifer Cetta, John F. Cox, William D. Freedman, Jennifer Kostyu, Jonathan Levi, Elisa Metzger, Iris Rosario, and Nadja Sodos-Wallace. Our thanks especially to John F. Cox for his contributions to this article.

1. Olmstead v. United States, 277 U.S. 438 (1928).
2. *Id.* at 466.
3. *Id.* at 476.
4. *Id.* at 478.
5. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

laws to implement the Court's holdings. These statutes in some respects set minimum standards for wiretaps by state officials. In other respects, however, the states retain considerable discretion in whether and how they will conduct wiretaps and other electronic surveillance.

The importance of state wiretaps comes in part from their volume. According to the most recent Wiretap Report of the Administrative Office of the United States Courts, at least sixty-seven percent of wiretap applications approved in 2001 were authorized by state judges (1,005 of 1,491).[6] Even more remarkably, while applications approved by federal judges in 2001 increased only one percent from the number authorized in 2000, approvals by state judges rose forty-one percent.[7]

Beyond mere volume, state legislatures have recently considered numerous proposals to alter wiretap and electronic surveillance law. The nature of these proposals is of particular interest in light of the USA PATRIOT Act, which was passed in the wake of the September 11 attacks.[8] The USA PATRIOT Act contains "sunset" provisions so that some of the new surveillance powers are scheduled to expire in the fall of 2005.[9] As Congress considers whether to extend or modify those surveillance powers, it will be useful to see how state legislators have been addressing the same issues.

The volume and diversity of state wiretap law and practice has not been accompanied by corresponding scrutiny. At the federal level, academics, the press, advocacy groups, and Congressional oversight have all provided important checks on any temptation by federal officials to overstep the limits of their surveillance powers. By contrast, we have not found any significant recent research on the law and practice of state wiretaps and other electronic surveillance.[10]

Even more troubling to our understanding of state wiretaps, it appears that some states may be failing to meet their obligation to report their wiretapping activity to the federal government. The 2001 Wiretap Report of the Administrative Office of the United States Courts says that forty-six jurisdictions have laws permitting the

6. ADMIN. OFFICE OF THE U.S. COURTS, THE 2001 WIRETAP REPORT 7 (2002), *available at* http://www.uscourts.gov/wiretap01/contents.html. Because of the likely under-reporting of state wiretaps, the percentage of state wiretaps is likely even higher.

7. *Id.* Of the 1,491 surveillance applications made to state and federal judges in 2001, not one was rejected. *Id.*

8. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA PATRIOT Act].

9. *Id.* § 224.

10. For an earlier study of state wiretap practices, which found serious and pervasive weakness in judicial control of state wiretaps, see generally SAMUEL DASH ET AL., THE EAVESDROPPERS (1959).

issuance of interception orders, but that judges from only twenty-five states reported using that authority in 2001.[11] Although it is possible that twenty-one states issued no interception orders in that year, it seems more likely that states are failing to make the required reports. Additional evidence of under-reporting is the mismatch between reports from state courts and prosecutors; the Wiretap Report in 2001 identified at least thirty-five wiretaps that were reported by state courts but not, as mandated by law, by prosecutors.[12]

To help fill the gaps in our knowledge, the research in this article was done under the umbrella of the Liberty and Security Initiative of the Constitution Project.[13] The Initiative was launched in the fall of 2001 as a bipartisan effort to study and seek consensus on issues affecting liberty and security after September 11. The research on state wiretap and electronic surveillance was done by the Privacy and Technology Committee of the Initiative. Professor Peter Swire serves as the academic reporter for this research.[14] Charles Kennedy is the project leader at the law firm of Morrison & Foerster LLP, which has contributed research on a pro bono basis.

Part I of the Article sets forth the constitutional and statutory framework for state wiretap and electronic surveillance law. Part II presents the key results from the study of the laws in the fifty states. Detailed reports on each state are and will remain available on the Internet.[15] The results here discuss the highlights of state wiretap and electronic surveillance legislation that has been proposed and enacted since September 11. The detailed reports also describe the key wiretap and electronic surveillance provisions in each state. Part III discusses implications and conclusions.

I. State Wiretap Laws: The Constitutional and Statutory Framework

Colonial Americans were acutely aware of the risks posed by physical searches of homes, offices, and other private places, and physical seizures of persons, papers, and other effects. These physical intrusions by the government were squarely addressed in the Fourth Amendment to the United States Constitution. The Twentieth Century, however, saw the use of mechanical and electronic devices that could capture private communications even where the police performed no physical trespass. The lack of a trespass was of key

11. 2001 WIRETAP REPORT, *supra* note 6, at 7.

12. *Id.* at 9.

13. *See* http://www.constitutionproject.org.

14. Professor Jeffrey Rosen of the George Washington University Law School serves as the reporter for Privacy and Technology Committee research on video surveillance.

15. *See* http://peterswire.net/pssurv.html.

doctrinal importance in *Olmstead*, leading the majority there to decide that there was no constitutionally protected "search."[16] The 1967 decision of *Katz v. United States* shifted the Fourth Amendment focus to "people, not places."[17] Since *Katz*, the central doctrinal question for surveillance has been whether an individual has a "reasonable expectation of privacy" in a particular communication.[18]

Our survey of state law addresses three basic categories of investigative techniques. The first category is where those doing the surveillance listen in to the content of the communications. Police or others might learn the content of communications by means of electronic eavesdropping, or bugging. This eavesdropping is typically accomplished by placing a listening device in or near an area where targeted conversations are likely to take place. These devices acquire the conversations in their acoustic, rather than electronic, form. The devices record the conversations or transmit them to law enforcement personnel at a listening post or other location. The police or others can also learn the content of communications by means of wiretaps, which intercept the content during the course of electronic transmission over a radio or wireline facility. Since *Katz*, the courts have applied the "reasonable expectation of privacy standard" to bugging and wiretaps to determine whether a Fourth Amendment "search" has occurred.[19] In this Article, we will use the term "wiretaps" to refer generically to wiretaps and bugging.

A second category is where police or others learn the "to/from" information of communications. The term "pen register" is used to refer to the list of telephone numbers, e-mail addresses, or similar information that receives a communication from the target of the investigation. The term "trap-and-trace device" is used where communications are traced back to their source, such as the phone number from which a call is made. The Supreme Court held in 1979 that this to/from information, under the facts of that case, was not subject to a "reasonable expectation of privacy."[20] This to/from information has thus not been subject to the probable cause standard of the Fourth Amendment.

The third category concerns records stored in the hands of third parties, such as banks, telephone companies, and Internet service providers. The Supreme Court has held that the Fourth Amendment does not prevent third parties from voluntarily turning over the

16. Olmstead v. United States, 277 U.S. 438, 466 (1928).
17. 389 U.S. 347, 351 (1967).
18. *Id.* at 360, 362 (Harlan, J., concurring).
19. *Id.*
20. Smith v. Maryland, 442 U.S. 735, 740 (1979).

stored records to law enforcement.[21] In our modern world, where the content of so much sensitive personal information is held by third parties, law enforcement officials can often learn about content or to/from information from stored records rather than by intercepting a call or e-mail as it occurs.[22]

The legal framework for these three categories of state laws is subject to two important constraints: first, the Fourth Amendment to the United States Constitution, as incorporated in and made applicable to the states by the Fourteenth Amendment; and second, the restrictions of federal statutes such as the Electronic Communications Privacy Act ("ECPA").[23]

The Fourth Amendment was first applied to state-ordered electronic surveillance by the Supreme Court in 1967. In *Berger v. New York*, the Court found New York's eavesdropping statute to be constitutionally defective because it did not require a showing of probable cause before an eavesdropping order would issue, and did not require specification of the crime that had been or was being committed and of the particular conversations being sought.[24] The statute also suffered other constitutional infirmities, because it authorized orders of excessive duration; did not require orders to be promptly executed; permitted extensions of the original eavesdropping period without a showing of probable cause; did not require termination of the eavesdropping once the conversation sought was seized; did not require a showing of "exigency" to justify use of eavesdropping as an investigative technique; and did not require a return of the warrant.[25]

The *Berger* decision gave the states a detailed guide to compliance with the Fourth Amendment in their use of eavesdropping and wiretap techniques. After *Berger*, states were on

21. United States v. Miller, 425 U.S. 435 (1976); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 54 (1974).

22. The pervasiveness of stored records, and the lack of constitutional protection against law enforcement access to such records, has been the subject of increasing attention. For instance, one of the authors (Professor Swire) chaired a White House Working Group in 2000 on how to update wiretap and surveillance laws for the Internet. In a speech announcing the Clinton Administration's legislative proposal, Chief of Staff John Podesta stressed the changed circumstances when e-mails and so many other sorts of personal communications are likely available in storage in the hands of third parties. Remarks by President's Chief of Staff John D. Podesta on Electronic Privacy to National Press Club (July 18, 2000), *in* FDCH FEDERAL DEPARTMENT AND AGENCY DOCUMENTS. For a recent scholarly discussion of the issue, see Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

23. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

24. Berger v. New York, 388 U.S. 41, 54–55, 58–59 (1967).

25. *Id.* at 59–60.

notice that their surveillance statutes and practices must ensure "adequate judicial supervision" and "protective procedures."[26] Specifically, orders must be issued by a judge, upon a showing of probable cause, with specification of the crime committed or about to be committed and the conversation or conversations to be seized.[27] Issuance of an order must be based upon a showing of circumstances that justify the use of the intrusive techniques of interception or eavesdropping.[28] The orders must be for a limited time and subject to a requirement of prompt execution.[29] Extensions of an order must be based upon probable cause, and the order must be returnable to the court to ensure judicial supervision of the order's execution.[30]

These constraints were codified and made more specific in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[31] "Title III," as it is generally called, established substantive and procedural requirements for federal interception orders.[32] It also specifically preempted less restrictive state requirements.[33] In 1986, Congress updated those requirements by means of the Electronic Communications Privacy Act, which addressed newer communications technologies such as mobile telephones and electronic mail.[34] (For convenience, we refer generically to the requirements of Title III and the ECPA as "ECPA requirements.")

The ECPA broadly prohibits all interceptions of the contents of wire, oral, and electronic communications, except where those interceptions comply with the ECPA requirements.[35] Where interceptions will be made by law enforcement agencies, the ECPA specifies the officials who may apply for an order, the crimes or categories of crimes in connection with which an order may be sought, the probable cause showing that the applicant must make, and the findings and "minimization" requirements that the order must contain.[36] The ECPA also requires state and federal courts issuing interception orders to make detailed reports concerning those orders to the Administrative Office of the United States Courts.[37] The ECPA also sets forth standards for pen register and trap-and-trace

26. *Id.* at 60.
27. *Id.* at 54–59.
28. *See id.* at 54–63.
29. *See id.* at 57–60.
30. *See id.* at 59–60.
31. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510–21 (2000)), *reprinted in* 1968 U.S.C.C.A.N. 237.
32. *Id.* §§ 2510–20.
33. *Id.* § 2515.
34. 18 U.S.C. §§ 2510–21 (2000).
35. *Id.* § 2511.
36. *Id.* § 2516–18.
37. *Id.* § 2519.

orders, and for government access to stored records held by third parties.[38]

Under the Fourth Amendment and ECPA constraints, states that wished to perform wiretaps were required to enact statutes that closely track the probable cause, minimization and other requirements of federal law. As we discuss further below, however, it is less clear that the states' institutional frameworks for electronic surveillance are as fully developed or protective of civil liberties as the federal regime.

II. Survey of State Wiretap Laws and Post-September 11 Amendments

Our research so far has resulted in the preparation and publication of two multi-page matrices. One matrix, titled *State Wiretap Legislation*, summarizes the legislative initiatives undertaken by several states in the initial period after the attacks of September 11, 2001.[39] The other matrix, titled *State Wiretap Laws*, summarizes the provisions of state statutes for wiretaps, to/from information, and stored records, including those that have not been amended since September 11, 2001.[40] Both matrices are and will be available on the Internet.[41]

We have found that most states (exceptions are noted on the second matrix) have enacted wiretap statutes. Not surprisingly, we have found that much of the post-September 11 legislation liberalizes, or proposes to liberalize, the state wiretap and other electronic surveillance laws. The chief categories of recently proposed changes include: expanding the list of offenses in connection with which interception orders may be granted; expanding the list of officials who may request wiretaps; expanding the categories of persons who may execute wiretaps; authorizing "roving" surveillance and surveillance across broader geographic areas; and expanding the types of communications and devices subject to interception.

38. *Id.* §§ 3121–27, 2701–11.

39. *See* Appendix A, *infra* page 987.

40. See Appendix B, *infra* page 1163.

41. In addition to their publication here, the matrices, including possible updates, are available at http://www.peterswire.net/pssurv.html, http://www.mofo.com/practice/ArticleDetail.cfm?MCatID=&concentrationID=&ID=938&Type=3, http://www.constitutionproject.org/ls/Summary_State_Chart_2_WDF_v1.DOC, and http://www.constitutionproject.org/ls/Chart_for_State_Wiretap_Legislation_v1.DOC.

A. Expanding the List of Offenses in Connection with Which Interception Orders May Be Granted

A number of amendments and proposed amendments to state laws add computer crimes and "terrorism," including various terrorism-related crimes, to the lists of offenses for which wiretap and similar authority may be granted.[42] These changes appear to be consistent with the requirements of the ECPA, which permits state interception orders in connection with

> the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.[43]

However, expansion of the state wiretap authority to include investigations of "terrorism" increases the likelihood of misuse of the surveillance power. Even at the federal level, where law enforcement has substantial experience with investigation of terrorist organizations, the loose statutory definitions of terrorism and terrorist-related activities, and the tendency of some officials to equate unpopular political expression with support for terrorism, have led to notorious abuses.[44] State authorities are less experienced in investigating "terrorism" and generally less subject to scrutiny from advocacy organizations, the press, and other outside groups. Expanded state investigations into "terrorism," therefore, could pose

42. S.B. 1427, 45th Leg., 2d Reg. Sess. (Ariz. 2002) (terrorist acts); A.B. 74, 2001–02 Reg. Sess. (Cal. 2002) (passed Sept. 17, 2002) (weapons of mass destruction and destructive devices, including "attempts" to commit those offenses); H.B. 5759, 2002 Gen. Assem., Reg. Sess. (Conn. 2002) (terrorism and computer crime in furtherance of terrorist purposes); H.B. 1439, 104th Reg. Sess. (Fla. 2002) (terrorism); H.B. 53A, 2002 1st Extraordinary Sess. (La. 2002) (terrorist acts); H.B. 100, 416th Gen. Assem., Reg. Sess. (Md. 2002) (unauthorized access to a computer); S.B. 184, 124th Gen. Assem., 2001–02 Sess. (Ohio 2001) (soliciting or providing support for an act of terrorism, making a terroristic threat, terrorism); H.B. 1120, 2002 Sess. (Va. 2002) (terrorism offenses); S.B. 514, 2002 Sess. (Va. 2002) (terrorism offenses).

43. 18 U.S.C. § 2516(2).

44. See, for example, the FBI's anti-terrorism investigation of the Committee In Solidarity with the People of El Salvador ("CISPES"), which resulted in legal action against, and admissions of wrongdoing by, the Bureau. Comm. in Solidarity with the People of El Salvador v. Sessions, 929 F.2d 742, 743–46 (D.C. Cir. 1991); Philip B. Heymann, *Civil Liberties and Human Rights in the Aftermath of September 11*, 25 HARV. J.L. & PUB. POL'Y 441, 444 (2002). *See generally* MORTON HALPERIN, ET AL., THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES (1976) (providing detailed history of illegal intelligence activities, which were often justified as necessary to combat Communist and other foreign threats).

significant risks of abuse, including abuse of First Amendment rights of free expression.

B. Expanding the List of Officials Who May Request Wiretap Authority

Under the ECPA, an application to a state court judge for an interception order must be made by the "principal prosecuting attorney of [the] State, or the principal prosecuting attorney of any political subdivision thereof."[45] The purpose of the requirement is the same as that of the counterpart ECPA requirement that federal applications be made by the Attorney General or designated persons responsible to the Attorney General, i.e., to centralize "in a publicly responsible official subject to the political process the formulation of [electronic surveillance policy so that s]hould abuses occur, the lines of responsibility lead to an identifiable person."[46]

State wiretap statutes vary widely in the degree of centralized decision-making they require. Some states permit applications to be made by a variety of officials, including county prosecutors.[47] Other states require that the application be preceded by the request or authorization of a central authority.[48]

To the extent we have seen recent legislative action concerning the officers that may request surveillance, the trend has been in the direction of dispersal rather than centralization of the power to bring such requests. Notably, a new Louisiana law expands, and a bill introduced in the Kentucky legislature would expand, the list of officials that may apply for wiretap orders.[49] Similarly, a bill introduced in the New York Assembly would add the chief counsel of a temporary state commission of investigation to the list of officials that may request a pen register or trap-and-trace order.[50]

C. Expanding the Categories of Persons Who May Execute Wiretaps

The training and competence of the persons who execute wiretap orders (sometimes called "monitors") are critical to the protection of the rights of subjects of surveillance. In addition to maintaining accurate activity logs (essential if there is to be any accountability for the way orders are implemented), monitors must be trained to minimize interceptions and discontinue monitoring when the

45. 18 U.S.C. § 2516(2).

46. S. REP. NO. 90-1097, at 97 (1968), *reprinted in* U.S.C.C.A.N. 2112, 2185.

47. *See, e.g.*, N.J. STAT. ANN § 2A:156A-8 (West 2003).

48. *See, e.g.*, TEX. CRIM. PROC. CODE ANN. art. 18.20 § 6 (Vernon 2003).

49. H.B. 53A, 2002 1st Extraordinary Sess. (La. 2002); H.B. 119, 2002 Reg. Sess. (Ky. 2002).

50. A.B. 5212, 224th Ann. Leg. Sess. (N.Y. 2001); S.B. 2156, 224th Ann. Leg. Sess. (N.Y. 2001).

intercepted conversation is privileged or not probative of crime.[51] For federal wiretaps, federal agents receive extensive training to comply with the detailed requirements under Title III and the ECPA.[52]

Under the ECPA, state-authorized interceptions may be carried out only by "investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made."[53] However, the ECPA permits private contractors to conduct interceptions, so long as the contractor's personnel are "under the supervision of an investigative or law enforcement officer authorized to conduct the interception."[54] The statutory authority to hire contractors for surveillance duty frees professional law enforcement personnel from the drudgery of staffing monitoring stations, but complicates the task of ensuring that persons who conduct surveillance are experienced and properly trained in the intricacies of executing an electronic surveillance order.

After September 11, 2001, a number of state legislatures expanded, or proposed to expand, the kinds of personnel who may conduct surveillance pursuant to interception orders. For example, Idaho now permits a wiretap to be conducted "by government personnel or by an individual operating under a contract with federal, state or local government and acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception."[55] In Illinois, the legislature has proposed to define "electronic criminal surveillance officer" to include retired law enforcement officers certified by the Department of State Police to intercept private oral communications.[56]

D. Authorizing "Roving" and Statewide Surveillance

Earlier wiretaps generally applied to a specific phone line. After September 11, states are increasingly introducing legislation to authorize "roving" wiretaps—i.e., orders that permit surveillance of any communications device a target of an investigation is likely to

51. S. REP. NO. 99-541, at 30–31, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3584–85.

52. For training materials used by the Department of Justice, see, for example, COMPUTER CRIME AND INTELL. PROP. SEC., CRIM. DIVISION, U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIM. INVESTIGATIONS (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (on file with the *Hastings Law Journal*); OFFICE OF ENFORCEMENT OPERATIONS, CRIM. DIVISION, U.S. DEP'T OF JUST., ELECTRONIC SURVEILLANCE MANUAL (1991) (on file with the Catholic University of America Law Library).

53. 18 U.S.C. § 2516(2).

54. *Id.* § 2518(5).

55. S.B. 1349, 56th Leg., 2d Reg. Sess. (Idaho 2002).

56. H.B. 4074, 92d Gen. Assem., Reg. Sess. (Ill. 2003).

use, without specifying the telephone or other facilities in the orders or applications.

Roving wiretaps have been permitted for years under the ECPA, which authorizes a court to order such an interception upon a showing that the target of the investigation is changing communication devices frequently and that this conduct "could have the effect of thwarting" the investigation.[57] Until recently, that procedure was not available for investigations under the Foreign Intelligence Surveillance Act ("FISA"). The USA PATRIOT Act harmonized the two statutes by extending roving wiretap authority to foreign intelligence investigations.[58] In the aftermath of September 11, a number of bills in the state legislatures also proposed to remove statutory restrictions on use of roving wiretaps by law enforcement.

Maryland's new statute, for example, permits "roving" orders for the interception of wire, oral and electronic communications.[59] For wiretaps, a "roving" order is permitted if the application: (1) is by an officer; (2) is approved by the attorney general, the state prosecutor, or a state's attorney; (3) identifies the person committing the offense and whose communications are to be intercepted; (4) makes a showing of probable cause that the person could thwart the interception from the facility; and (5) specifies that the interception will be limited to any period of time in which the officer has a reasonable, articulable belief that the suspect will be using those facilities.[60]

Similarly, bills introduced in the Minnesota and New York legislatures would permit roving wiretaps as a means of intercepting communications of persons suspected of terrorist activity;[61] and legislation was introduced in Wisconsin that would have permitted roving wiretaps.[62]

57. 18 U.S.C. § 2518(11)(b)(ii). Roving wiretaps were authorized for domestic surveillance in 1986, in the Electronic Communications Privacy Act, § 106(d)(3), 100 Stat. at 1857 (1986). In 1998, the 105th Congress amended the roving wiretap statute and reduced the *mens rea* requirement for requesting authorities from cases in which the target had a "purpose . . . to thwart interception by changing facilities," 18 U.S.C. § 2518(11)(b)(ii) (1997), to cases in which the suspect's actions "could have the effect of thwarting interception from a specified facility." Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998). For a critical discussion of the amendment of the roving wiretap statute, see Bryan R. Faller, *The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better*, 60 OHIO ST. L.J. 2093 (1999).

58. USA PATRIOT Act §206 (2001), 15 Stat. 272, 282 (2001).

59. H.B. 100, 416th Gen. Assem., Reg. Sess. (Md. 2002).

60. *Id.*

61. H.B. 2909, 82d Leg. Sess. (Minn. 2001); S.B. 5793, 225th Ann. Leg. Sess. (N.Y. 2001).

62. S.B. 363, 95th Leg. Sess, (Wis. 2001–02).

A number of states have also followed the federal lead in authorizing interceptions outside of the geographic bounds of the court's normal jurisdiction. Under the USA PATRIOT Act, federal judges may now issue a pen register/trap-and-trace order that applies nationwide, rather than only in the district in which the judges sit.[63] In Florida, if an applicant demonstrates that an act involves or will involve terrorism, a judge may now authorize an interception for anywhere in the state even if beyond the jurisdictional bounds of the court.[64] Similarly, in Idaho, wiretap authorization now extends beyond the issuing court's territorial jurisdiction to include the entire state.[65]

In Maryland, a judge may authorize continued interception throughout the state if the original interception occurred within the judge's jurisdiction.[66] The definition of an authorizing judge is expanded to include circuit courts having jurisdiction over the crime being investigated, regardless of the location of the instrument or process from which a wire or electronic communication is transmitted or received.[67] Finally, in Virginia, the amendments to the wiretap statute remove physical location and geographic boundary requirements from wiretap applications.[68]

Statutory grants of extraterritorial wiretap jurisdiction, in particular, may dilute the ability and incentive of courts to exercise effective control over the surveillance process. The possibilities for abuse include law enforcement "judge shopping" and reduction of the court's ability to supervise wiretaps that are executed in various counties outside the court's jurisdiction.[69]

E. Expanding the Types of Communications and Devices Subject to Interception

A number of bills propose to add new devices and types of communications to those susceptible of authorized interception by law enforcement. These include electronic communications,

63. USA PATRIOT Act § 216(a), 115 Stat. at 288.

64. H.B. 1439, 104th Reg. Sess. (Fla. 2002).

65. S.B. 1349, 56th Leg., 2d Reg. Sess. (Idaho 2002).

66. H.B. 1036, 416th Gen. Assem., Reg. Sess. (Md. 2002); S.B. 639, 416th Gen. Assem., Reg. Sess. (Md. 2002).

67. H.B. 1036, 416th Gen. Assem., Reg. Sess. (Md. 2002); S.B. 639, 416th Gen. Assem., Reg. Sess. (Md. 2002).

68. H.B. 1120, 2002 Sess., (Va. 2002); S.B. 514, 2002 Sess., (Va. 2002).

69. For a discussion of the provision to permit judges to issue orders nationwide, as well as other electronic surveillance provisions in the USA PATRIOT Act, see Peter P. Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, Brookings Terrorism Project Website, *at* http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm (Oct. 3, 2001), *also available at* http://www.peterswire.net.

voicemail, cordless telephones, cellular telephones and stored communications.[70]

These developments are not alarming in themselves. In adding new devices and technologies to their wiretap statutes, states generally are bringing their laws in line with the ECPA, which for many years has applied to non-wireline and non-voice communications not addressed in older wiretap statutes. Extension of surveillance activities to any new technology, however, may present challenges to which the training and experience of state and local courts and law enforcement personnel may not be adequate.

III. Conclusions and Suggestions for Further Research

Most wiretaps in the United States are performed by state officials, yet almost all of the scrutiny of wiretap practices has applied to the federal level. An appreciation of state law and practice is thus central to understanding the enforcement of the privacy rights of individuals in their telephone calls, e-mails, and other communications. In the research performed for the Constitution Project, we have systematically described the interception, to/from, and stored record laws that existed in the states as of June 1, 2002. This research shows the diversity of state laws and provides a baseline so that interested persons over time can determine with relatively minimal research the laws that apply in their own states.

One result of our research has been for us to consider the meaning of the federal minimum standards provided by the Electronic Communications Privacy Act and related statutes. At a formal level, the ECPA provides that state wiretap and other laws may have effect only if they meet the federal requirements for nature of the offense, minimization, and so on. We believe, however, that there are two significant ways in which the protection of rights under state wiretaps is often less effective than for federal wiretaps.

First, the institutional setting varies for federal and state surveillance. For federal law enforcement, institutional safeguards and training of personnel have achieved a high degree of sophistication. Federal wiretap requests generally are the result of internal agency vetting, approval from the prosecuting Assistant United States Attorney, approval from the Department of Justice's Office of Enforcement Operations, and approval by a high-level Department of Justice official. Only then is the application submitted to a district court judge for approval. The Office of Enforcement

70. S.B. 459, 146th Gen. Assem., Reg. Sess. (Ga. 2002); S.B. 1349, 56th Leg., 2d Reg. Sess. (Idaho 2002); H.B. 2986, 79th Leg., Reg. Sess. (Kan. 2002); A.B. 1589, 24th Ann. Leg. Sess. (N.Y. 2001–02); H.B. 1120, 2002 Sess. (Va. 2002); S.B. 514, 2002 Sess. (Va. 2002).

Operations, in particular, acts as a repository of federal wiretap judgment and expertise that can check any missteps by less experienced prosecutorial personnel. Federal law enforcement personnel that execute wiretap orders also receive a high level of training.

Institutions, procedures and training at the state level are less well understood. Some states do permit only the state police to request and administer wiretaps. Some state law enforcement agencies have expert departments with the ability to screen proposed uses of surveillance techniques that are unlawful and inappropriate, and trained operatives that can reliably execute wiretaps within the limits of the interception orders. Other states, however, permit local police agencies to request and carry out wiretaps. Prosecutors may seek wiretaps who are often less fully supervised than is true in the federal system. Based on our review of state laws, we consider it likely that state wiretaps are often less subject to institutional controls on prosecutorial and police discretion.

This lack of internal institutional controls is matched by a relative lack of external controls on the discretion and actions of state officials. Few states have their actions subjected to the same scrutiny on civil liberties grounds that academics and numerous groups in Washington, D.C. give to proposed and actual federal actions. Media attention to federal activities is greater. State legislatures and their judiciary committees often lack the staffing and expertise of the judiciary committees in the U.S. Congress. It is likely, in addition, that the Congressional committees display greater ongoing vigilance on the activities of the U.S. Department of Justice than is true for many state legislatures, which often meet for limited sessions.

Because state procedures are watched less systematically by the press and civil liberties organizations, abuses at the state level, whether deliberate or the result of inexperience, may not be detected. The under-reporting of state wiretaps, discussed above, is both a symptom of and a contributing factor to this relative lack of oversight. The simple fact is that half of the states have wiretap powers, yet reported no wiretaps in 2001. The utter failure to file the annual wiretap report would be unthinkable at the federal level. In addition, the under-reporting of state wiretaps keeps the use and possible misuse of state wiretaps less visible.

At a policy level, the twin phenomena of weaker internal and external controls argue for greater public oversight of state wiretap practices. Courts and prosecutors who do not file wiretap reports should be brought to light. States that provide wiretap authority to prosecutors and police, without effective training or oversight, should consider how to bring their practices up to a higher level. Watchdog groups and the media, armed with the database about the actual laws

in the fifty states, can ask more useful questions about how wiretaps and related surveillance actually operate in each state.

A separate implication of this research concerns the interplay of federal and state surveillance law. Based on the authors' own experience, the debate on the USA PATRIOT Act in the fall of 2001 focused essentially exclusively on the scope of surveillance powers that is appropriate for federal officials. The preemption provision in the ECPA, however, means that a change in federal law also permits an equivalent change in state law. Many of the bills recently proposed or enacted in the states mirror the reduction of privacy rights in the USA PATRIOT Act. For topics such as the definition of "terrorist" crimes, the use of roving wiretaps, and the use of surveillance orders statewide, the states are "catching up" to the changes at the federal level.

In the abstract, there is no simple way to determine whether these changes to state laws are desirable. Where the change in federal law is desirable, an equivalent change in state law may also be desirable. The weakness of internal and external controls at the state level, however, throws an additional element into the mix. A change in federal law, it turns out, has two effects: a change in the law as applied by federal officials; and permission to the states to expand their surveillance activities as well. This dual effect deserves the attention of Congress as it revisits the surveillance powers that are subject to the sunset provision in the USA PATRIOT Act. Even where sufficient controls can be created to justify actions by federal officials, there should be additional inquiry. Can the controls be, and will they be, created at the state level where the large majority of wiretaps actually occur? The actual effects of legal changes, and potential for abuse, may lurk more in the state systems than we have suspected.

***