

An Overview of the Law of Electronic Surveillance Post September 11, 2001*

Robert A. Pikowsky**

Mr. Pikowsky examines the significance of the USA PATRIOT Act, enacted in the wake of the September 11 terrorist attacks, on the law of electronic surveillance. He discusses the likely effects of the Act on universities and libraries.

Table of Contents

Introduction	602
A Very Brief History of Wiretapping.	602
Modern Statutory Regulation of Wiretapping during Domestic Criminal Investigations.	604
Interception of Telephone Calls before the USA PATRIOT Act.	604
Statutory Treatment of E-mail and Voicemail before the USA PATRIOT Act	606
Pen Registers and Trap and Trace Devices before the USA PATRIOT Act.	608
USA PATRIOT Act Amends the Law Governing Wiretaps, Access to Stored Communication, and Pen Registers	608
Modern Statutory Regulation of Wiretapping and Physical Searches during Foreign Intelligence Investigations	611
Electronic Surveillance and Physical Searches Pursuant to the Foreign Intelligence Surveillance Act before the USA PATRIOT Act	611
Pen Registers and Trap and Trace Devices Pursuant to the Foreign Intelligence Surveillance Act before the USA PATRIOT Act	614
Access to Business Records Pursuant to the Foreign Intelligence Surveillance Act before the USA PATRIOT Act	614
USA PATRIOT Act Amends the Foreign Intelligence Surveillance Act. . .	614
Modern Statutory Protection of Educational Records	616
Access to Educational Records before USA PATRIOT Act Amendments	616
USA PATRIOT Act Amends the Family Educational Rights and Privacy Act	616
Impact of the USA PATRIOT Act on Educational Institutions and Libraries	617

* © Robert A. Pikowsky, 2002.

** Electronic Services Law Librarian, University of Idaho Law Library, Moscow, Idaho.

Introduction

¶1 Since its enactment by Congress in the wake of the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon, there has been much publicity about the USA PATRIOT Act.¹ The Act made numerous amendments to existing statutes governing covert electronic surveillance pursuant to the investigation of domestic crimes as well as investigations concerning foreign intelligence and terrorism. Critics have argued that the Act will unduly increase the power of government to conduct electronic surveillance at the expense of civil liberties.²

¶2 In order to understand the significance of the USA PATRIOT Act to the law of electronic surveillance, it is necessary to have some familiarity with the history of the law of wiretapping prior to its enactment. This article will summarize the evolution of the law of wiretapping, beginning with early case law and extending to the statutory environment at the time the USA PATRIOT Act was enacted.³ It will then go on to examine some of the numerous technical amendments imposed by the USA PATRIOT Act upon the existing statutes governing electronic surveillance. Lastly, it will discuss the effects of the USA PATRIOT Act on universities and libraries, concluding that the impact will not be as great as some have feared.

A Very Brief History of Wiretapping

¶3 The first wiretapping case decided by the Supreme Court was *United States v. Olmstead*.⁴ Federal prohibition agents suspected Olmstead of violating the National Prohibition Act. They overheard incriminating conversations by setting up a wiretap to intercept telephone calls between Olmstead and his attorney. The district court allowed the prosecution to introduce evidence of those conversations. Olmstead was ultimately convicted. On appeal, the Ninth Circuit Court of Appeals agreed that the wiretap evidence was admissible. The Supreme Court held that the wiretap was not subject to Fourth Amendment restrictions because it was established without any physical intrusion into the homes or offices of the defendants. Moreover, no physical objects were seized. Thus, neither a search nor a seizure had taken place. In his famous dissent, Justice Brandeis argued for recognition of a

-
1. 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 [hereinafter USA PATRIOT Act].
 2. *E.g.*, *The USA Patriot Act of 2001: Electronic Surveillance and Privacy*, 6 Electronic Com. & L. Rep. (BNA) No. 46, at 1206 (Dec. 5, 2001) (citing material on the Web sites of the American Civil Liberties Union, the Center for Democracy & Technology, and the Electronic Frontier Foundation).
 3. The areas of law discussed in this article are fairly complex. In providing a brief overview, this article will necessarily omit some details of the statutes. As a result, some principles of law may be oversimplified for the sake of brevity.
 4. 277 U.S. 438 (1928).

right to be let alone so that “every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.”⁵

¶4 The *Olmstead* majority noted that Congress could “protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus, depart from the common law of evidence.”⁶ Subsequently, Congress enacted the Communications Act of 1934. Section 605 prohibited anyone from intercepting communications covered by the statute and disclosing their contents unless authorized by the sender.⁷

¶5 Section 605 greatly limited the use of wiretap evidence in federal court. But federal officials continued to conduct wiretaps associated with foreign intelligence investigations on the rationale that the statute did not entirely prohibit such activities when national security was involved. The FBI continued to conduct wiretaps in furtherance of domestic crime investigations based on the argument that section 605 did not prohibit wiretapping, but only prohibited wiretapping followed by “divulgence.”⁸ The Department of Justice took the position that information had not been divulged when a governmental official passed the information on to another.⁹

¶6 By the 1960s, the Supreme Court began to reevaluate its ruling in *Olmstead*. The Court came to recognize that a search could take place without a physical trespass upon a person’s property.¹⁰ This principle was firmly established in 1967 by *Katz v. United States*,¹¹ where the Court adopted the standard by which the extent of Fourth Amendment protections are still measured today. In *Katz*, the FBI attached a listening device to the exterior of a phone booth without a search warrant in order to eavesdrop on the defendant’s side of telephone conversations regarding illegal gambling activities. The defendant was convicted at trial based in part on tape recordings obtained through that listening device. The Supreme Court reversed the conviction because the government had violated the privacy upon which the defendant justifiably relied and thereby conducted a search and seizure even in the absence of a physical trespass.¹²

¶7 Also in 1967, the Supreme Court struck down a New York statute setting out an ex parte procedure by which law enforcement officials could obtain judicial authorization to establish telephone wiretaps. In *Berger v. New York*,¹³ the Court

5. *Id.* at 478 (Brandeis, J., dissenting).

6. *Id.* at 465–66.

7. Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1103–04 (codified as amended at 47 U.S.C. § 605 (2000)).

8. 2 WAYNE R. LAFAVE, JEROLD H. ISRAEL, & NANCY J. KING, CRIMINAL PROCEDURE § 4.1(b), at 328–29 (2d ed. 1999).

9. *Id.*

10. *Id.* § 4.2(c), at 330–31.

11. 389 U.S. 347 (1967).

12. *Id.* at 348.

13. 388 U.S. 41 (1967).

held that the statute violated the Fourth and Fourteenth Amendments for seven separate reasons:

- the statute did not require the search warrant to sufficiently describe the crime under investigation;
- the statute did not require a sufficiently “precise and discriminate” description of the conversations that the police wanted to monitor;
- the statute authorized eavesdropping for an extended period of time that was deemed to violate the requirement of prompt execution;
- the statute permitted extension of the time period without sufficient showing of probable cause for the continuation;
- the statute did not require termination of the eavesdropping when the police overheard the conversation they were waiting for;
- the statute did not require a showing of exigent circumstances which are necessary to overcome the secrecy and lack of notice that are necessarily associated with wiretapping; and
- the statute lacked any provision for a return of service on the warrant to account for the records of conversations that had been overheard.¹⁴

¶8 While the Supreme Court was reevaluating *Olmstead*, it had become clear that law enforcement needed greater latitude to employ wiretaps than was permitted by section 605. In 1967, the Supreme Court decisions in *Katz* and *Berger* provided new guidance as to constitutionally acceptable procedures under which evidence obtained through wiretapping could be introduced as evidence in court. The following year, a new statutory scheme governing wiretaps was enacted.¹⁵

Modern Statutory Regulation of Wiretapping during Domestic Criminal Investigations

Interception of Telephone Calls before the USA PATRIOT Act

¶9 Congress responded to *Berger* by enacting the Federal Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968.¹⁶ This shifted the focus away from the Federal Communications Act of 1934 in order to strike a new balance between the right to privacy and the needs of law enforcement. The Federal Wiretap Act went so far as to include statutory protections beyond the constitutional protections that were articulated in *Berger*.

¶10 As originally enacted, the Federal Wiretap Act generally prohibited the willful interception of wire (primarily telephone) or oral communications.¹⁷ The

14. *Id.* at 55–60.

15. 2 LAFAYE, ISRAEL, & KING, *supra* note 8, § 4.2(c), at 331–32.

16. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 212–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)).

17. § 802, 82 Stat. at 213–14 (current version at 18 U.S.C. § 2511 (2000)).

Act granted power to the attorney general, deputy attorney general, and several other officials to seek judicial authorization to conduct a telephone wiretap during the investigation of certain specifically listed crimes.¹⁸ It also granted similar power to state officials.¹⁹

¶11 The Act delineated the circumstances in which a judge could issue an interception order.²⁰ These provisions are summarized by LaFave, Israel, and King:

An interception order may be issued only if the judge determines on the basis of facts submitted that there is probable cause for belief that an individual is committing, has committed, or is about to commit one of the enumerated offenses; probable cause for belief that particular communications concerning that offense will be obtained through such interception; that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and probable cause for belief that the facilities from which, or the place where, the communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. Each interception order must specify the identity of the person, if known, whose communications are to be intercepted; the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; a particular description of the type of communication sought to be intercepted; and a statement of the particular offense to which it relates; the identity of the agency authorized to intercept the communications and of the person authorizing the application; and the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. No order may permit interception “for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days.” Extensions of an order may be granted for like periods, but only by resort to the procedures required in obtaining the initial order.²¹

¶12 Before long, the Federal Wiretap Act’s definitions of oral and wire communications led the courts to struggle with the treatment of intercepted conversations over portable telephones and mobile telephones (the predecessor of cellular telephones). In 1986, the Electronic Communications Privacy Act amended the Federal Wiretap Act to include cellular telephone conversations within the restrictions placed on wiretapping.²² However, the Electronic Communications Privacy Act expressly excluded the broadcast portion of portable telephone conversations from its statutory protection.²³ In 1994, the Communications Assistance for Law Enforcement Act further amended the Federal Wiretap Act to prohibit the

18. § 802, 82 Stat. at 216–17 (current version at 18 U.S.C. § 2516(1) (2000)).

19. § 802, 82 Stat. at 217 (current version at 18 U.S.C. § 2516(2) (2000)).

20. § 802, 82 Stat. at 218–21 (current version at 18 U.S.C. § 2518 (2000)).

21. 2 LAFAVE, ISRAEL, & KING, *supra* note 8, § 4.2(a), at 333 [citations omitted].

22. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(a)(1)(B), 100 Stat. 1848, 1848 (amending 18 U.S.C. § 2510(1) (1982)).

23. § 101(a)(1)(D), 100 Stat. at 1848 (amending 18 U.S.C. § 2510(1) (1982)).

unauthorized interception of the broadcast portion of portable telephone conversations.²⁴

Statutory Treatment of E-mail and Voicemail before the USA PATRIOT Act

¶13 The Electronic Communications Privacy Act made significant revisions to the regulations governing wiretaps. It amended the Federal Wiretap Act so that it would also govern the interception of “electronic communication.” Accordingly, the interception of e-mail has come to be regulated in a manner similar in many respects to the regulation of telephone conversations. But there are important distinctions. For example, the statutory exclusionary rule applicable to unlawfully intercepted telephone conversations²⁵ is inapplicable to unlawfully intercepted e-mail. Moreover, a wider range of federal officials can seek judicial authorization to intercept e-mail than are permitted to seek judicial approval of interception of telephone conversations.²⁶ And e-mail can be intercepted as part of the investigation of any federal felony.²⁷

¶14 Title II of the Electronic Communications Privacy Act also added a series of statutory sections that are commonly known as the Stored Communications Act.²⁸ These provisions govern access to e-mail held in electronic storage for the recipient at an Internet Service Provider (ISP). Thus, the statutes draw a distinction between interception of e-mail while in transmission and access to that same communication once it has reached its destination and is held in the recipient’s mailbox.

¶15 The Stored Communications Act generally prohibits intentional unauthorized access to an “electronic communications facility” in order to obtain an electronic communication (e-mail message) held in electronic storage.²⁹ The statute requires the government to obtain a search warrant in order to compel an ISP to disclose the contents of an e-mail message held in electronic storage for 180 days or less.³⁰ Prior or contemporaneous notice to the subscriber is not necessary. The Stored Communications Act provides less protection for e-mail held in electronic

24. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202(a)(1), 108 Stat. 4279, 4290 (1994) (amending 18 U.S.C. § 2510(1) (1988)). To be more precise, the Act did not expressly prohibit the unauthorized interception of the broadcast portion of portable telephone conversations. Rather, it deleted language from the Federal Wiretap Act that excluded the broadcast portion from its protections against unlawful interception.

25. 18 U.S.C. § 2515 (2000). In the absence of a statutory exclusionary rule, illegally obtained evidence may be admissible in court under the good faith exception to the constitutional exclusionary rule. See Michael Lieb, *E-mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III’s Statutory Exclusionary Rule and Expressly Reject a “Good Faith” Exception*, 34 HARV. J. LEGIS. 393 (1997).

26. Compare 18 U.S.C. § 2516(1) (2000) with 18 U.S.C. § 2516(3) (2000).

27. 18 U.S.C. § 2516(3).

28. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2711 (2000)).

29. 18 U.S.C. § 2701.

30. 18 U.S.C. § 2703.

storage more than 180 days.³¹ As an alternative to a search warrant, the government can compel the ISP to disclose the contents of e-mail through an administrative subpoena or court order if prior notice is given to the subscriber. But the statute provides for the possibility of delayed notice as well.

¶16 The distinctions between the Federal Wiretap Act and the Stored Communications Act make clear that law enforcement officials must meet a higher burden in seeking authorization to intercept an e-mail message during transmission than in seeking authorization to access that same message the moment after it reaches the recipient's mailbox. There is little case law interpreting this aspect of the statutes, but one would expect law enforcement officials to routinely tailor their investigative techniques to access stored e-mail rather than to intercept e-mail in transmission.³²

¶17 Surprisingly, the FBI's proprietary electronic surveillance software, originally named "Carnivore" but now renamed "DCS1000," operates as a packet sniffer that reads e-mail on an ISP's network while still in transmission. This software has been the subject of heated debate because of the potential for abuse by law enforcement agents. Concern has been raised about its capability to read all e-mail on the network without limitation to e-mail sent to or from the target of a judicially authorized search.³³ Nevertheless, federal law enforcement has developed technology that invokes the greater protections of the Federal Wiretap Act in favor of alternatives that would be governed by the lesser protections of the Stored Communications Act.

¶18 Until recently, both the Federal Wiretap Act and the Stored Communications Act contained provisions governing access to voicemail by law enforcement officials. Surprisingly, these provisions were mutually inconsistent. Before the USA PATRIOT Act amendments, the Federal Wiretap Act defined "wire communication" so as to include the electronic storage of a wire communication.³⁴ This language would arguably bring voicemail under the protections of the Federal Wiretap Act and require the government to meet the Act's relatively high standards in order to obtain search authorization.

¶19 But the Stored Communications Act also brought wire communications in electronic storage under its provisions.³⁵ So one could argue that voicemail merely received the lesser protections of the Stored Communications Act, in which case the government would only be required to meet the relatively lower standard of that Act in order to obtain a search warrant.

31. *Id.*

32. *See* Steve Jackson Games v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994) (unlawful seizure of a computer that operated an electronic bulletin board system containing unread e-mail in the recipients' mailboxes does not constitute interception under the Federal Wiretap Act).

33. Rachel Konrad, *New Documents Shed More Light on FBI's "Carnivore,"* CNET News.com, at <http://news.cnet.com/news/0-1005-202-3731884.html> (Nov. 16, 2000).

34. 18 U.S.C. § 2510(1) (2000).

35. 18 U.S.C. § 2701.

¶20 The Ninth Circuit has held that access to voicemail is governed by the Federal Wiretap Act.³⁶ But as will be seen, the USA PATRIOT Act amended the statutory scheme and unambiguously brought voicemail under the Stored Communications Act. Whether this lesser standard complies with the requirements of *Berger* will need to be settled by the courts.

Pen Registers and Trap and Trace Devices before the USA PATRIOT Act

¶21 A pen register is a device attached to a telephone line to covertly record any outgoing telephone numbers that are dialed. Pen registers do not monitor or record the content of telephone calls. Similarly, a trap and trace device records the telephone number from which an incoming call originates.

¶22 Neither pen registers nor trap and trace devices are governed by the Federal Wiretap Act because they do not intercept the content of telephone conversations.³⁷ Nor are they governed by the Fourth Amendment because a person making a telephone call has no reasonable expectation of privacy in the telephone number dialed since this information is of necessity revealed to the telephone company in order to make the call.³⁸

¶23 In 1986, the Electronic Communications Privacy Act placed some minimal limitations on the use of pen registers and trap and trace devices by law enforcement officials. It required a court to approve the installation of a pen register or a trap and trace device based on a request by the appropriate federal or state officials who certify only “that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”³⁹ Since the Supreme Court had already ruled that the implementation of pen registers or trap and trace devices by law enforcement officers did not amount to a wiretap for purposes of the Federal Wiretap Act or a search for purposes of Fourth Amendment analysis, it is not surprising that Congress set a rather relaxed standard by which judicial authorization could be obtained.

***USA PATRIOT Act Amends the Law Governing Wiretaps,
Access to Stored Communication, and Pen Registers***

¶24 In the aftermath of September 11, Congress enacted the USA PATRIOT Act, making extensive revisions to the existing statutes governing covert surveillance of wire and electronic communications. The full name of the Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) is somewhat misleading in that some of its revisions apply to the investigation of domestic criminal offenses that are entirely

36. United States v. Smith, 155 F.3d 1051 (9th Cir. 1998).

37. United States v. N. Y. Tel. Co., 434 U.S. 159, 165–68 (1977).

38. Smith v. Maryland, 442 U.S. 735, 740–46 (1979).

39. 18 U.S.C. § 3123(a) (2000).

unrelated to terrorist activities. Selected revisions⁴⁰ are discussed in the following sections of the article.

¶25 Section 202 of the USA PATRIOT Act amends existing law⁴¹ to authorize interception of telephone conversations or e-mail during the investigation of felony violations of the Computer Fraud and Abuse Act. Previously, such offenses were not included in the list of crimes for which law enforcement officers could obtain judicial authorization to conduct a wiretap. However, this amendment will sunset on December 31, 2005.

¶26 Section 209 of the USA PATRIOT Act⁴² amends provisions of the Federal Wiretap Act⁴³ and the Stored Communications Act⁴⁴ to clear up the ambiguity about which governs access to voicemail. Law enforcement officers can now obtain judicial authorization for access to voicemail pursuant to the lesser requirements of the Stored Communications Act. This amendment will sunset on December 31, 2005.

¶27 Section 210 of the USA PATRIOT Act amends the Stored Communications Act provision⁴⁵ regarding government access to information about anyone who subscribes to a telephone company or an ISP. Prior law expressly authorized the government to obtain such information as subscriber name, address, telephone number, and telephone toll billing records through issuance of a subpoena. The statutory language had become outdated in that it used terminology that was primarily applicable to telephone communications. Section 210 of the Act adds such matters as credit card or bank account number. It also makes clear that information pertaining to Internet use (such as Internet protocol addresses and session times) can be obtained in addition to information pertaining to telephone communications.

¶28 Section 211 of the USA PATRIOT Act amends the Cable Act provision⁴⁶ governing government access to customer records possessed by cable service providers. The Cable Act was initially enacted to preserve the privacy of customers who bought television programming through cable companies. Accordingly, prior law set a very high burden on law enforcement officers who sought judicial authorization to view records held by cable companies. But today cable companies also offer telephone service and Internet access. Section 211 brings the Cable Act in line with the Federal Wiretap Act and the Stored Communications Act with regard to telephone service and Internet access.

40. Other revisions governing such matters as money laundering and immigration are beyond the scope of this article.

41. USA PATRIOT Act, Pub. L. No. 107-56, § 202, 115 Stat. 272, 278 (2001) (amending 18 U.S.C. § 2516(1) (2000)).

42. § 209, 115 Stat. at 283.

43. 18 U.S.C. § 2510(1) (2000).

44. 18 U.S.C. § 2703 (2000).

45. § 210, 115 Stat. at 283 (amending 18 U.S.C. § 2703(c) (2000)).

46. § 211, 115 Stat. at 283–84 (amending 47 U.S.C. § 551 (2000)).

¶29 Section 212 of the USA PATRIOT Act amends sections of the Stored Communications Act⁴⁷ concerning emergency disclosures by ISPs. Section 212 permits ISPs to voluntarily disclose the content of subscriber communications and information about a subscriber if it discovers information pertaining to immediate risk of death or serious physical injury. This amendment will sunset on December 31, 2005.

¶30 Section 216 of the USA PATRIOT Act amends the law governing pen registers and trap and trace devices.⁴⁸ Much of the prior law was drafted with reference to conventional telephones. The revised language makes clear that law enforcement officials can obtain analogous information concerning e-mail, such as Internet protocol addresses.

¶31 Moreover, section 216 gives national effect to an order authorizing a pen register or trap and trace device. In other words, an order issued by a court having jurisdiction over the crime under investigation can authorize the implementation of a pen register or trap and trace device in other districts as necessary.⁴⁹ Therefore, law enforcement officers no longer have to seek orders from multiple courts in the course of large-scale investigations.

¶32 Lastly, section 216 expands the definitions of pen register⁵⁰ and trap and trace device⁵¹ to include software as well as mechanical devices. It requires law enforcement officers who use their agency's equipment or software to establish the pen register or trap and trace device (rather than relying on the communication provider) to provide a report to the court under seal detailing certain information about their activities.⁵²

¶33 Section 217 of the USA PATRIOT Act amends a provision of the Federal Wiretap Act⁵³ so as to permit an ISP to seek assistance from law enforcement officers in investigating the activities of a "computer trespasser." The new law enables the ISP to authorize law enforcement officers to monitor communications to or from the trespasser, but they cannot monitor the communications of authorized users. Even with authorization, law enforcement officers can monitor communications only when they have reasonable grounds to believe that the communications are relevant to the investigation. This amendment will sunset on December 31, 2005.

¶34 Section 220 of the USA PATRIOT Act amends the Stored Communications Act⁵⁴ to give nationwide effect to search warrants authorizing law enforcement officers to obtain stored e-mail held in a subscriber's mailbox by an ISP. Previously the Federal Rules of Criminal Procedure limited the scope of a search

47. § 212, 115 Stat. at 284–85 (amending 18 U.S.C. §§ 2702–03 (2000)).

48. § 216, 115 Stat. at 288–90 (amending 18 U.S.C. §§ 3121(c), 3123(a), 3123(b)(1), 3123(d)(2), 3124(b), 3124(d), 3127(1)–(4) (2000)).

49. § 216(b)(1), 115 Stat. at 288–89 (amending 18 U.S.C. § 3123(a) (2000)).

50. § 216(c)(2), 115 Stat. at 290 (amending 18 U.S.C. § 3127(3) (2000)).

51. § 216(c)(3), 115 Stat. at 290 (amending 18 U.S.C. § 3127(4) (2000)).

52. § 216(b)(1), 115 Stat. at 288–89 (amending 18 U.S.C. § 3123(a) (2000)).

53. § 217(2), 115 Stat. at 291 (amending 18 U.S.C. § 2511 (2000)).

54. § 220, 115 Stat. at 291–92 (amending 18 U.S.C. § 2703 (2000)).

warrant to property within the district of the court that issued the warrant.⁵⁵ The new law permits a court with jurisdiction over the offense being investigated to issue a search warrant for stored e-mail held by an ISP anywhere in the country. Thus, law enforcement officials do not need to seek a warrant in the jurisdiction where the ISP's server happens to be located. This amendment will sunset on December 31, 2005.

¶35 Section 505 of the USA PATRIOT Act amends the Stored Communications Act provision governing FBI access to customer records held by a wire or electronic communication service provider as it applies to counterintelligence investigations.⁵⁶ Prior law permitted the FBI to order the service provider to turn over records containing the name, address, and length of service, as well as local and long distance toll billing records pursuant to a counterintelligence investigation. The FBI was not required to seek prior judicial authorization to obtain this information. Rather, the FBI needed only to certify to the service provider that the information was "relevant to an authorized foreign counterintelligence investigation" and that there were "specific and articulable facts" giving reason to believe that the information pertained to a foreign power or an agent of a foreign power.⁵⁷ Similar statutory provisions were applicable to investigations involving international terrorism.⁵⁸

¶36 Section 505 lessens and simplifies the certification that the FBI must give to the service provider. Now the FBI need only certify that the records are relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

Modern Statutory Regulation of Wiretapping and Physical Searches during Foreign Intelligence Investigations

*Electronic Surveillance and Physical Searches Pursuant to the
Foreign Intelligence Surveillance Act before the USA PATRIOT Act*

¶37 The federal courts have recognized the power of the president to order electronic surveillance without prior judicial authorization during the investigation of matters concerning foreign intelligence.⁵⁹ This authority was codified by the Foreign Intelligence Surveillance Act⁶⁰ (FISA) in 1978. FISA was amended in 1994 to expressly permit the execution of warrantless covert physical searches.⁶¹

55. FED. R. CRIM. P. 41.

56. § 505, 115 Stat. at 365 (amending 18 U.S.C. § 2709 (2000)).

57. 18 U.S.C. § 2709(b)(1).

58. 18 U.S.C. § 2709(b)(2).

59. *United States v. Truong*, 629 F.2d 908, 912-16 (4th Cir. 1980). See William Michael, *A Window on Terrorism: The Foreign Intelligence Surveillance Act*, BENCH & B. MINN., Nov. 2001, at 23.

60. Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-1829 (2000)).

61. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 807(a)(3), § 302, 108 Stat. 3423, 3444-46 (1994) (codified as amended at 50 U.S.C. § 1822 (2000)).

¶38 FISA permits the president, through the attorney general, to authorize electronic surveillance to acquire foreign intelligence information without judicial approval under limited circumstances when that surveillance targets the content of communications that are “transmitted by means of communications used exclusively between or among foreign powers.”⁶² FISA expressly prohibits warrantless electronic surveillance unless there is no substantial likelihood that the surveillance will acquire the contents of a communication to which a U.S. citizen or permanent resident is a party.⁶³

¶39 Similarly, FISA permits the president, through the attorney general, to authorize a physical search to acquire foreign intelligence information without judicial approval under limited circumstances when the search targets “premises, information, material, or property used exclusively by . . . a foreign power or powers.”⁶⁴ FISA expressly prohibits a warrantless physical search unless there is no substantial likelihood that the search will involve the property of a U.S. citizen or permanent resident.⁶⁵

¶40 In other circumstances, prior judicial authorization is necessary to conduct electronic surveillance or to perform a physical search. FISA established a special court to review requests for such authorization. The court originally consisted of seven U.S. district court judges selected from seven judicial circuits by the Chief Justice of the Supreme Court.⁶⁶ A review panel consists of three additional judges selected by the Chief Justice to hear appeals from the denial of a request for authorization.⁶⁷ In the event that the appeal is also denied, the government can bring the matter to the Supreme Court through a petition for writ of certiorari.⁶⁸

¶41 To obtain a FISA warrant for electronic surveillance, federal officials must submit an application that, *inter alia*, identifies the target of the surveillance⁶⁹ and states facts indicating that the target is a foreign power or an agent of a foreign power.⁷⁰ Further, the application must state facts indicating that the facilities to be monitored are being used by a foreign power or an agent of a foreign power.⁷¹ The application must describe the information that is sought to be uncovered⁷² and explain the minimization procedures that will be followed.⁷³ The application must contain a certification that federal officials are seeking “foreign intelligence information”⁷⁴ that cannot reasonably be obtained by normal investigative

62. 50 U.S.C. § 1802(a)(1)(A)(i).

63. 50 U.S.C. § 1802(a)(1)(B).

64. 50 U.S.C. § 1822(a)(1)(A)(i).

65. 50 U.S.C. § 1822(a)(1)(A)(ii).

66. 50 U.S.C. § 1803(a); 50 U.S.C. § 1822(c).

67. 50 U.S.C. § 1803(b); 50 U.S.C. § 1822(d).

68. 50 U.S.C. § 1803(b); 50 U.S.C. § 1822(d).

69. 50 U.S.C. § 1804(a)(3).

70. 50 U.S.C. § 1804(a)(4)(A).

71. 50 U.S.C. § 1804(a)(4)(B).

72. 50 U.S.C. § 1804(a)(6).

73. 50 U.S.C. § 1804(a)(5).

74. 50 U.S.C. § 1804(a)(7)(A).

techniques⁷⁵ and must state the basis for that certification.⁷⁶ Under current procedures, the Justice Department Office of Intelligence Policy and Review supervises the preparation of applications for FISA warrants and represents the United States before the FISA court.⁷⁷

¶42 The FISA court is to approve electronic surveillance if it makes the findings required by statute. These findings include, *inter alia*, the existence of probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power as well as probable cause to believe that the facilities where the surveillance is to be directed are being used by a foreign power or an agent of a foreign power.⁷⁸

¶43 However, the court is not required to find probable cause to believe that the surveillance will actually uncover foreign intelligence information. In this regard, the standard for issuance of a FISA warrant is lower than the standard for issuance of a search warrant in a domestic criminal investigation.⁷⁹

¶44 The statutory provisions for obtaining a warrant to conduct a covert physical search roughly parallel the provisions for obtaining a warrant to conduct electronic surveillance. To obtain a FISA warrant to conduct a physical search, federal officials must submit an application that, *inter alia*, identifies the target of the investigation and describes the property to be searched.⁸⁰ The application must state facts indicating that the target is a foreign power or an agent of a foreign power and that the property to be searched contains foreign intelligence information.⁸¹ The application must also explain the minimization procedures to be employed during the search.⁸² The application must contain a certification that federal officials are seeking “foreign intelligence information”⁸³ that cannot reasonably be obtained by normal investigative techniques⁸⁴ and must state the basis for that certification.⁸⁵

¶45 The FISA court is to approve a physical search if it makes the findings required by statute. These findings include, *inter alia*, the existence of probable cause to believe that the target of the search is a foreign power or an agent of a foreign power, as well as probable cause to believe that the property to be searched is being used by a foreign power or an agent of a foreign power.⁸⁶

75. 50 U.S.C. § 1804(a)(7)(C).

76. 50 U.S.C. § 1804(a)(7)(E).

77. 28 C.F.R. § 0.33b (2002); U.S. DEP’T OF JUSTICE, UNITED STATES ATTORNEY’S MANUAL § 1-2.106 (1997); Michael, *supra* note 59, at 23–24.

78. 50 U.S.C. § 1805(a)(3).

79. 2 LAFAVE, ISRAEL, & KING, *supra* note 8, § 4.3(d), at 364–65.

80. 50 U.S.C. § 1823(a)(3).

81. 50 U.S.C. § 1823(a)(4).

82. 50 U.S.C. § 1823(a)(5).

83. 50 U.S.C. § 1823(a)(7)(A).

84. 50 U.S.C. § 1823(a)(7)(C).

85. 50 U.S.C. § 1823(a)(7)(E).

86. 50 U.S.C. § 1824(a)(3).

Pen Registers and Trap and Trace Devices Pursuant to the Foreign Intelligence Surveillance Act before the USA PATRIOT Act

¶46 Prior to the USA PATRIOT Act, federal officials were permitted to seek approval from the FISA court for installation of a pen register or trap and trace device during an FBI investigation to gather foreign intelligence information or information concerning international terrorism.⁸⁷ The application was required to certify, inter alia, that the information likely to be obtained is relevant to an ongoing FBI investigation under guidelines approved by the attorney general.⁸⁸ And the application had to provide information demonstrating a reason to believe that the telephone line or other means of communication to be monitored is being used by an individual engaged in international terrorism or clandestine intelligence activities that may violate U.S. criminal law.⁸⁹ An order approving installation of a pen register or trap and trace device had to specify the identity of the target of the investigation, if known, as well as the telephone number (or corresponding information applicable to other means of communication) to be monitored.⁹⁰

Access to Business Records Pursuant to the Foreign Intelligence Surveillance Act before the USA PATRIOT Act

¶47 Prior to enactment of the USA PATRIOT Act, FISA permitted the director of the FBI or his designee to apply to the FISA court for an order directing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release its records to assist the FBI in gathering foreign intelligence information or in investigating international terrorism.⁹¹ The application had to specify that there were specific and articulable facts giving reason to believe that the records pertain to a foreign power or an agent of a foreign power. No employee of an organization releasing records pursuant to an order of the FISA court could reveal that the FBI had demanded those records except to other employees as necessary to accomplish the task.⁹²

USA PATRIOT Act Amends the Foreign Intelligence Surveillance Act

¶48 Section 206 of the USA PATRIOT Act amends existing law to permit “roving wiretaps.”⁹³ Previously, an order from a FISA court authorizing electronic surveillance was required to direct a specified communications carrier to help set up the surveillance if so requested in the application for the order. But naming a particular carrier in the order becomes impracticable where the target of the investigation

87. 50 U.S.C. § 1842(a)(1) (2000).

88. 50 U.S.C. § 1842(c)(2).

89. 50 U.S.C. § 1842(e)(3).

90. 50 U.S.C. § 1842(d)(2).

91. 50 U.S.C. § 1862(a) (2000).

92. 50 U.S.C. § 1862(d)(2).

93. USA PATRIOT Act, Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001) (amending 50 U.S.C. § 1805(b)(2)(B) (2000)).

may employ multiple cellular telephones, conventional telephones, e-mail accounts, or other means of communication. Section 206 allows the FISA court order to omit the names of individual carriers where the court finds that the “actions of the target . . . may have the effect of thwarting the identification” of the carriers. The result is that surveillance can “follow a person, rather than requiring a separate court order identifying each telephone company or other communication common carrier whose assistance is needed.”⁹⁴ This provision will sunset on December 31, 2005.

¶49 Section 208 of the USA PATRIOT Act expands the FISA court from seven to eleven judges, at least three of whom are to reside in the vicinity of Washington, D.C.⁹⁵

¶50 Section 214 of the USA PATRIOT Act amends the FISA provisions concerning pen registers and trap and trace devices.⁹⁶ This statute previously required that the application for authorization to implement a pen register or trap and trace device must provide information demonstrating a reason to believe that the line to be monitored was being used by an individual engaged in international terrorism or clandestine intelligence activities that may violate U.S. criminal laws.⁹⁷ This requirement is repealed; it is now sufficient that the application certifies that the information likely to be obtained is foreign intelligence information not concerning a U.S. citizen or permanent resident, or that the information likely to be obtained is relevant to an investigation to protect against international terrorism.

¶51 It would appear that the statutory amendment lessens the burden on law enforcement officials seeking to establish a pen register or trap and trace device. As amended, the statute no longer requires a factual showing in support of the request for judicial authorization. However, the amended certification requirement provides greater assurances that foreign intelligence surveillance will not pertain to a U.S. citizen or permanent resident. Section 214 will sunset on December 31, 2005.

¶52 Section 215 of the USA PATRIOT Act amends the FISA provisions concerning orders to turn over business records to the FBI.⁹⁸ Prior law was applicable only to common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. Section 215 removes the limitations on the type of business that must comply with the order, so that anyone can be required to produce tangible things including books, records, papers, documents, and other items. The government need only specify that the records sought contain foreign intelligence information not concerning a U.S. citizen or permanent resident. Alternatively, the government may specify that the records are needed to protect against international terrorism. This provision will sunset on December 31, 2005.

94. 147 CONG. REC. S10998 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

95. § 208, 115 Stat. at 283 (amending 50 U.S.C. § 1803 (2000)).

96. § 214, 115 Stat. at 286–87 (amending 50 U.S.C. § 1842 (2000)).

97. 50 U.S.C. § 1842(c)(3) (2000).

98. § 215, 115 Stat. at 287–88 (amending 50 U.S.C. §§ 1861–1863 (2000)).

¶53 Section 218 of the USA PATRIOT Act amends statutory provisions concerning the application for a FISA warrant authorizing electronic surveillance or a physical search.⁹⁹ These provisions required the application to include, inter alia, a certification that the purpose of the surveillance or search is to obtain foreign intelligence information. However, the purpose may include criminal prosecution as well. Some courts resolved this ambiguity by interpreting the statute to require only that the primary purpose was to obtain foreign intelligence information.¹⁰⁰ Section 218 relaxed this interpretation even further by changing the statutory language to require only that “a significant purpose” is to obtain foreign intelligence information. This provision will sunset on December 31, 2005.

Modern Statutory Protection of Educational Records

Access to Educational Records before USA PATRIOT Act Amendments

¶54 Federal statutes create a strong economic incentive for universities to maintain the privacy of records pertaining to their students. The Family Educational Rights and Privacy Act (FERPA) generally provides that no funds will be made available to an educational institution that permits the release of educational records of its students (or personally identifiable information beyond directory information contained in a record) except where the release is authorized by the student or by statute.¹⁰¹

¶55 FERPA permits the release of information to appropriate parties in an emergency if necessary to protect the health or safety of the student or others.¹⁰² FERPA also makes clear that student information can be disclosed without prior consent pursuant to a court order or subpoena.¹⁰³ However, the institution must make a reasonable effort to notify the student of the order or subpoena so that the student can seek protective action before information is released. But the law is somewhat different when a federal grand jury subpoena or any other subpoena for law enforcement purposes is served on a university. The court issuing the subpoena, for good cause shown, can order the institution not to reveal the existence of the subpoena. If so ordered, the institution must abide by the instructions to maintain the secrecy of the subpoena.

USA PATRIOT Act Amends the Family Educational Rights and Privacy Act

¶56 Section 507 of the USA PATRIOT Act amends FERPA by adding a new subsection that allows certain federal officials designated by the attorney general to

99. § 218, 115 Stat. 291 (amending 50 U.S.C. §1823(a)(7)(B); 50 U.S.C. § 1804(a)(7)(B) (2000)).

100. *E.g.*, *United States v. Sarkissian*, 841 F.2d 959, 964–65 (9th Cir. 1988).

101. Family Educational Rights and Privacy Act, Pub. L. No. 93-380, § 513 88 Stat. 571 (codified at 20 U.S.C. § 1232g (2000)).

102. 20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. § 99.36 (2002).

103. 20 U.S.C. § 1232g(b)(1)(J); 34 C.F.R. § 99.31(9)(i) (2002).

seek an ex parte order from any court of competent jurisdiction to obtain educational records during an investigation of domestic or international terrorism, or other specified crimes. The court must grant the order if the application certifies that there are specific and articulable facts giving reason to believe that the education records are likely to contain information relevant to the investigation.¹⁰⁴ Significantly, it would appear that the certification is sufficient to obtain the order without actually informing the court of the underlying facts.

Impact of the USA PATRIOT Act on Educational Institutions and Libraries

¶57 The USA PATRIOT Act enhances the ability of law enforcement officials to implement electronic surveillance during domestic criminal investigations as well as intelligence investigations. For example, the Act clarifies prior statutory language and lessens the standard that law enforcement officers must meet when requesting a search warrant for voicemail messages. The Act also authorizes the operator of a computer network to permit electronic surveillance of activity by a “computer trespasser.” Nevertheless, the provisions of the Act regarding the vast majority of domestic criminal investigations do not have a uniquely troubling impact on universities or libraries beyond their impact on society as a whole.

¶58 The concern has been expressed that a university could be sued if it asks the FBI for assistance in tracking down an intruder on its network.¹⁰⁵ As previously discussed, the USA PATRIOT Act permits the FBI to read the contents of e-mail sent to or from a computer trespasser if an ISP requests assistance in investigating the trespasser’s activities. Nevertheless, the intruder might argue in court that the provisions of the statute allowing electronic surveillance without a search warrant violate the Fourth Amendment. If so, then the university might be exposed to liability for facilitating an illegal search.

¶59 In this scenario, the potential liability of a university is no different than the potential liability of any other business entity. The possibility that a computer trespasser could recover damages is very unlikely because the trespasser would find it difficult to establish that he had a reasonable expectation of privacy in the unauthorized account he had set up on the university’s computer.

¶60 A more serious concern involves the scenario where FBI agents contact university officials with information about a suspected computer trespasser and ask for permission to investigate the trespasser’s activities.¹⁰⁶ University officials may grant permission due to a desire to cooperate with law enforcement and to maintain the security of the university’s computer network, or they may be afraid

104. § 507, 115 Stat. at 367–68 (amending 20 U.S.C. § 1232g (2000)).

105. Scott Carlson & Andrea L. Foster, *Colleges Fear Anti-Terrorism Law Could Turn Them Into Big Brother*, CHRONICLE HIGHER EDUC., Mar. 1, 2002, at 31.

106. *Id.*

to deny permission. Although it is unlikely that a computer trespasser could recover damages, the true danger is the possibility that university officials may be intimidated into granting permission in the absence of judicial oversight. In the event that law enforcement officers are aggressive in their efforts to investigate computer trespassers, university officials will need to decide whether they are willing to cooperate or whether they must decline to permit electronic surveillance within their computer network.

¶61 But there is little reason to believe that law enforcement officials will suddenly rely on the USA PATRIOT Act amendments to coerce university officials into permitting electronic surveillance within the university's network. Prior law had already been interpreted so as to allow the operator of a network that is not open to the general public to release the contents of e-mail messages. *Andersen Consulting v. UOP*¹⁰⁷ held that a private corporation providing e-mail accounts for its employees was not liable for releasing the contents of e-mail to the *Wall Street Journal*. The court reasoned that the corporation was not obligated by the Stored Communications Act to protect the privacy of e-mail accounts on its network because this aspect of the statute applied only to the operators of networks that are available to the general public.

¶62 Since only employees and students (but not the general public) can open accounts on a university's computer network, universities arguably had the authority to release the contents of e-mail under the prior law subject only to the university's obligations to those employees and students. In view of this case law, universities were already exposed to the actions of aggressive law enforcement officers before enactment of the USA PATRIOT Act. However, it is true that the new statutory language could further embolden law enforcement officers.

¶63 It should be recognized that any statutory amendments lessening the burden on law enforcement officials seeking to conduct electronic surveillance could pose a constraint on the academic freedom of university faculty. This is particularly true where faculty take unpopular positions on matters involving foreign affairs and might be subject to investigation under FISA. But many of the FISA provisions expressly limit searches or surveillance involving a U.S. citizen or permanent resident. Moreover, FISA provisions expressly recognize First Amendment rights.¹⁰⁸

¶64 Of course, the USA PATRIOT Act amendments to FERPA will uniquely impact universities in some respects. The amendments set a very low standard to be met by law enforcement officers seeking a judicial order for the production of student educational records. Fortunately, these amendments are generally limited to investigations involving domestic or international terrorism.

107. 991 F. Supp. 1041 (N.D. Ill. 1998).

108. *E.g.*, 50 U.S.C. § 1861(a)(2)(B) (2000) (providing that an FBI request for a FISA court order to obtain business records will be denied if the investigation of a U.S. citizen or permanent resident is based solely on activities protected by the First Amendment).

¶65 As far as libraries are concerned, there is little reason to believe that the FBI will aggressively suggest that libraries should request assistance in tracking down computer trespassers pursuant to the USA PATRIOT Act. Unlike universities operating high bandwidth networks that make them prime targets for hackers, few libraries operate networks that are likely to attract the interest of hackers. Therefore, it is unlikely that situations will often develop where trespassers in library networks will come to the attention of federal law enforcement officials.

¶66 However, the USA PATRIOT Act amendments to FISA, while not expressly targeting libraries, apparently will decrease the privacy of client records in limited circumstances. The amendments permit the FBI to obtain an order directing the production of business records without a factual showing and without limitation on the type of business entity that must comply.¹⁰⁹ Thus, library records of materials checked out by clients and library records of Internet activity may be subject to search and seizure insofar as they pertain to foreign intelligence or international terrorism. At present, it is too early to predict how aggressively the FBI will invoke the new provisions in seeking to conduct searches of library records. Because the holder of the records is forbidden to reveal that a search has taken place, it may be impossible to gather statistics on the number of searches that are conducted.

¶67 In any event, law enforcement requests for library records during the course of a terrorism investigation raise an interesting ethical issue. Libraries have traditionally tried to preserve the privacy of their clients. Circulation records are generally deleted when the borrowed item is returned. And generally no permanent records are kept of Internet browsing on library computers beyond the information that may continue to exist on the computer's hard drive incident to the operation of the computer.

¶68 Yet if a person uses his or her own computer to commit illegal acts, law enforcement may discover evidence by obtaining judicial authorization to search and seize that computer. Moreover, Web logs maintained at sites visited by the suspect may reveal such information as his or her IP address and other identifiable information unless he or she is using an anonymous browsing service such as anonymizer.com.

¶69 But when a suspect uses a public computer in a library, it becomes more difficult to isolate and trace evidence of criminal activity to that specific individual. It is even more difficult if the library does not require its clients to sign in with their name, date, and time before they are allowed to use a computer.

¶70 Thus, a person who uses a library's public computer in support of criminal activity is afforded greater anonymity than someone who uses his own home computer. So the library administration must weigh the privacy of its clients against the need to obtain evidence of crime when setting policy governing maintenance and

109. § 215, 115 Stat. at 287–88; *see supra* ¶ 52.

retention of records. These competing factors must also be considered when characterizing the impact of the USA PATRIOT Act on libraries.

¶71 The USA PATRIOT Act made many technical amendments to the Federal Wiretap Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act. In actuality, libraries had been subject to the provisions of these statutes governing electronic surveillance prior to enactment of the USA PATRIOT Act, but the library community only recently became aware of the statutory environment in which it exists as a result of the publicity surrounding the new act. In that light, the USA PATRIOT Act did not have an unreasonable impact on the privacy of library clients; it merely awakened the library community to the issues of electronic surveillance that had already existed.