THE NEED FOR REVISIONS TO THE LAW OF WIRETAPPING AND INTERCEPTION OF EMAIL

*Robert A. Pikowsky**

Cite as: Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. TECH. L. REV. 1 (2003), *available at* http://www.mttlr.org/volten/pikowsky.pdf

* Technology Law Librarian/Associate Professor, University of Idaho. M.L.I.S., Rosary College Graduate School of Library and Information Science, 1995; J.D., University of Illinois College of Law, 1981; B.S. in Business Administration, University of Illinois College of Commerce and Business Administration, 1978.

I. INTRODUCTION

Communication over the Internet continues to grow in popularity among individuals and businesses. As the Internet becomes friendlier to casual users, computing technology is converging with telecommunications technology.[1] Cell phones incorporate email and web browsing

1. The convergence of these industries is well documented in the media. For example, a joint announcement in 1998 by Hewlett-Packard Co. and Cisco Systems detailed their plans to manufacture equipment for telephone companies that will integrate voice and data communications. Eventually, video may also be integrated into the network. Tom Quinlan, *Technology Deals Aim to Bring Together Voice, Data Networks,* SAN JOSE MERCURY NEWS, Nov. 2, 1998, at 1E; *see* Stephen Lee, *Voice Over IP gets Wake-Up Call,* INFOWORLD, May 4, 2001, *at* http://www.infoworld.com/articles/hn/xml/01/05/07/010507hnvoip.xml (last visited December 4, 2003).

Moreover, IBM, Intel, Toshiba, Nokia, and Ericsson have established a standard for wireless communication known as "Bluetooth," which is a computing and telecommunications industry description of the manner in which products such as personal computers, cellular phones, personal digital assistants, and other devices can interconnect using a short range wireless connection. Approximately 1,900 companies have adopted the Bluetooth standard. Chris Gaither, *Bluetooth Defies Obituaries*, N.Y. TIMES, December 20, 2001, at G5; Janet Rae-Dupree, *Bluetooth Lets Gadgets Speak in One Language*, U.S. NEWS & WORLD REPORT, May

capabilities, while Personal Digital Assistants feature cell phone functions. Meanwhile, Internet telephony enables users to conduct voice conversations between computers, between a computer and a telephone, or between telephones.[2]

The Federal Wiretap Act[3] generally prohibits the use of technology to intercept "oral" communication between people taking part in a face-to-face conversation, "wire" communication between parties to a telephone conversation, or "electronic" communication via computer. The Stored Communications Act[4] protects the privacy of wire and electronic communications held in electronic storage at an electronic communication service. The statutes set out the procedures that must be followed by law enforcement officials in order to obtain judicial authorization for monitoring these communications.

In drafting these statutes, Congress unduly focused on the different communications technologies rather than the common privacy interests that exist across all media of communication. As a result, different standards govern the issuance of judicial authorization for law enforcement officers to conduct a telephone wiretap, to intercept email, or to covertly access email from storage in a person's mailbox at his Internet Service Provider.

Complicating matters further, most of the statutory framework was in place before wireless telephone communications became commonplace and before the Internet became available to the general public. As telecommunications and computing technologies continue to advance and to converge with one another, the statutory scheme will become

---

15, 2000, at 58; Amy Doan, *Cutting the Cord*, FORBES, August 23, 1999, at 48; Whatis.com, *Bluetooth*, *at* http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=bluetooth (last visited November 9, 2003); *but see* Carmen Nobel, *Still Waiting for Bluetooth*, EWEEK, April 23, 2001, at 1.

Another recent event highlighting this convergence between technologies is the announcement of a new wireless handheld device based on an Intel chipset running the Microsoft Smartphone 2002 operating system. It will be able to make voice calls, send email, play music and video, take pictures, and keep a diary. The device is to be introduced in Europe by the end of the third quarter of 2003. *Wintel Teams Up With Taiwan's MiTAC, Unveils Smartphone*, THE ELECTRONIC TIMES (Korea), August 14, 2003, *available at* 2003 WL 4177042.

2. *See* Steve Bass, *Net Phones: Dialing Without Dollars*, PC WORLD, November 2000, *at* http://www.pcworld.com/reviews/article.asp?aid=18623 (last visited November 9, 2003). In Australia, a coalition of universities and research institutions is averaging 5,000 long distance calls per business day over the Internet at an estimated savings of 70–90 per cent. Geoffrey Maslen, *Australian Universities Use Internet for Long-Distance Calls*, THE CHRONICLE OF HIGHER EDUCATION, April 3, 2001, *at* http://chronicle.com/free/2001/04/2001040301t.htm (last visited November 9, 2003); *see* Florence Olsen, *Colleges Experiment with Routing On-Campus Phone Calls over the Internet*, THE CHRONICLE OF HIGHER EDUCATION, October 23, 2001, *at* http://chronicle.com/free/2001/10/2001102301t.htm (last visited November 9, 2003).

3. 18 U.S.C. §§ 2510–2522 (2000).

4. 18 U.S.C. §§ 2701–2711 (2000).

increasingly out of touch with the privacy expectations of the American public.

I argue that a person's privacy interest in his email is the same as his privacy interest in a telephone conversation. Moreover, the privacy interest in email remains unchanged regardless of whether it is intercepted in transmission or covertly accessed from the recipient's mailbox. If one accepts this assumption, it follows that the level of protection against surveillance by law enforcement officers should be the same.

However, inconsistencies in the Federal Wiretap Act and the Stored Communications Act lead to illogical distinctions in the treatment of wire and electronic communication. For example, fewer federal officials are empowered to seek authorization for a telephone wiretap than are empowered to seek authorization for the interception of email. With proper authorization, a telephone wiretap can be conducted only during the investigation of specifically enumerated federal crimes. However, email can be intercepted during the investigation of any federal felony. In the event of an unlawful telephone wiretap, telephone conversations are protected by a statutory exclusionary rule. In contrast, unlawfully intercepted email receives only the lesser protection of the constitutional exclusionary rule as limited by the "good faith" exception.

Until October 2001, voicemail received greater protection from police searches than was extended to email stored in the recipient's mailbox at his Internet Service Provider. Surprisingly, during the course of its transmission, email is afforded greater statutory protection against interception by the police than is extended to email stored in the recipient's mailbox. A federal district court recently held that a message remaining on the Internet Service Provider's server after it has been read by the intended recipient is no longer statutorily protected from unauthorized access.

Patricia M. Worthy correctly points out that Congress has consistently employed a technology-driven approach in protecting the privacy of telephone conversations as conventional wire telephones evolve into wireless devices.[5] An attempt by Congress to follow a similar approach with respect to communication via computer may prove to be unworkable due to the rapid pace of technological innovation. Worthy is correct in stating that "[t]he pace of technological change necessitates

5. As will be discussed later, the Federal Wiretap Act was amended in 1986 to extend its protections to cellular telephone conversations, while expressly excluding the radio portion of cordless telephone conversations from protection. The statute was amended again in 1994 to remove this exclusion. *See* Patricia M. Worthy, *The Impact of New and Emerging Telecommunications Technologies: A Call to the Rescue of the Attorney-Client Privilege*, 39 How L.J. 437, 448–54 (1996).

adopting legal reforms that are derived from a technology-neutral basis, and, therefore, are not rooted in current technology."[6]

As technology continues to blur the distinction between wire and electronic communication, it becomes apparent that a new methodology must be developed in order to provide logical and consistent protection to private communications. The statutes must be revised so as to protect the privacy of communications while also providing a means by which law enforcement officers can obtain judicial approval to eavesdrop when necessary. Otherwise, increasing integration between data and voice communications will render the current statutory scheme arbitrary and impractical.

By way of background, this article will discuss the law governing mail searches as well as the law of covert searches generally. This article will go on to discuss the regulation of pen registers, and will then trace the evolution of the relevant federal statutory and constitutional protections afforded to telephone conversations.

Next, this article will discuss the statutory protections and the emerging case law addressing the privacy of email and other communication via computer. Particular emphasis will be placed on several recent federal court decisions that illustrate the problems arising from the current statutory scheme.

Lastly, this article will discuss the controversial implementation of the FBI's "Carnivore" software for the purpose of surreptitiously intercepting email, and the recent deployment of a keystroke-logging device as another means of learning the contents of private electronic communications.

This article asserts that the Fourth Amendment protections applicable to telephone conversations set out by *Katz v. United States*[7] and *Berger v. New York*[8] (subsequently codified and expanded by the Federal Wiretap Act) should be implemented more broadly to encompass the surreptitious surveillance of postal mail, email, and other promising forms of electronic communication.[9] This article argues in favor of more uniform regulation of covert surveillance of private communications regardless of the choice of technology employed to convey the message.[10]

---

6. *Id.* at 471.

7. 389 U.S. 347 (1967).

8. 388 U.S. 41 (1967).

9. James X. Dempsey questions whether our traditional concepts of the Fourth Amendment remain valid in this context when "many of our most important records are not 'papers' in our 'houses,' but are 'bytes' stored electronically and accessed remotely at 'virtual' locations." James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 88–89 (1997).

10. The irrational distinctions in the treatment of various communications technologies were recognized in a 1994 law review comment by a student author calling for statutory

II. MAIL SEARCHES AND OTHER COVERT SEARCHES

A. *The Law of Mail Searches*

A mail search may be an isolated event limited to a single letter, or it may continue over an extended period of time so as to permit law enforcement officials to surreptitiously read an ongoing exchange of correspondence. This latter possibility poses a particularly grave threat to privacy unless closely supervised by the judiciary because the police carry out the search and seizure operation without giving contemporaneous notice to the correspondents. In this respect, the issues raised by mail searches are similar to those raised by telephone wiretaps. Regardless of the medium of communication, similar expectations of privacy are called into question when the police conduct a covert surveillance with judicial authority to delay notification to the person whose communications have been searched.

Ex Parte Jackson[11] is often cited for the proposition that letters placed in first class mail cannot be opened and read by law enforcement officers in the absence of a search warrant.[12] The Court stated that:

> [A] distinction is to be made between different kinds of mail matter, between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and

amendments. Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 251–52 (1994).

11. 96 U.S. 727 (1877).

12. *See* 4 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 10.3(b), at 467–68 (3d ed. 1996).

> all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the Fourth Amendment of the Constitution.[13]

Although the Court clearly stated that the protections of the Fourth Amendment are applicable to letters placed in the mail, this language was merely dicta. The Court went on to state that the only issue to actually be decided was the constitutionality of a statute prohibiting the mailing of certain letters intended to deceive the public and obtain money under false pretenses.[14] That statute was upheld and the underlying criminal conviction was allowed to stand.[15]

In deference to the strong policies favoring the privacy of first class mail, statutory and regulatory protections have been enacted. 39 U.S.C. § 3623(d) states:

> The Postal Service shall maintain one or more classes of mail for the transmission of letters sealed against inspection. The rate for each such class shall be uniform throughout the United States, its territories, and possessions. One such class shall provide for the most expeditious handling and transportation afforded mail matter by the Post Office. No letter of such a class of domestic origin shall be opened except under authority of a search warrant authorized by law, or by an officer or employee of the Postal Service for the sole purpose of determining an address at which the letter can be delivered, or pursuant to the authorization of the addressee.[16]

This language is echoed in 39 C.F.R. § 233.3(g)(1), which states:

> No person in the Postal Service except those employed for that purpose in dead-mail offices, may open, or inspect the contents of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise nonmailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute.[17]

In 1970, the Supreme Court considered the extent to which a package placed in the mail was protected from interception by the police in

13. *Ex Parte Jackson*, 96 U.S. at 733.

14. *Id.* at 736–37.

15. *Id.*

16. Similar language had previously appeared at 39 U.S.C. § 4057 (Supp. II 1959–1960). But mail originating outside of the United States may generally be searched pursuant to the more relaxed rules governing border searches. *See* 19 C.F.R. § 145.2; *see also* 4 LAFAVE, *supra* note 12, § 10.5(j), at 597–603.

17. 39 C.F.R. § 233.3(g)(1) (2003).

the absence of a search warrant. In *United States. v. Van Leeuwen*,[18] the Post Office delayed delivery of two suspicious packages for about a day while the police conducted an investigation and obtained a search warrant. The police then opened the packages, which contained gold coins that were imported in violation of 18 U.S.C. § 545.

The defendant's conviction in District Court was reversed by the Ninth Circuit.[19] On certiorari, the Supreme Court held that a delay of about 29 hours from the time the defendant mailed the packages until the search warrant was served did not violate the Fourth Amendment prohibition against unreasonable search and seizure.[20]

The Court reasoned that first class mail, such as letters and sealed packages subject to letter postage, is free from postal inspection except in accordance with the Fourth Amendment and that the detention of the package until a search warrant was obtained did not amount to an unreasonable seizure under the circumstances.[21]

It is significant to note that the defendant in *Ex Parte Jackson* was convicted of an offense based on the content of a letter. In contrast, the *Van Leeuwen* conviction was founded on the presence of a physical object. Yet Justice Douglas's opinion in *Van Leeuwen* acknowledged the possibility that mail searches can implicate First Amendment issues as well as Fourth Amendment issues,[22] thereby providing further reason to strictly safeguard the privacy of the mail.

An interesting discussion of mail searches can be found in *United States v. Rollack*.[23] There, the defendant was imprisoned for federal narcotics conspiracy charges prior to and during his trial. While he was in jail, federal agents seeking evidence of further crimes intercepted his incoming and outgoing mail over a period of nine days pursuant to a search warrant. The warrant waived the normal statutory requirement of contemporaneous notice of the search. Instead, delayed notice was authorized in order to avoid compromising the investigation. Continuation of the surreptitious mail search was authorized by

18. 397 U.S. 249 (1970).
19. *Id.* at 250.
20. *Id.* at 253.
21. *Id.*
22. In an apparent reference to *Ex Parte Jackson*, Justice Douglas explained:

> The course of events since 1878 has underlined the relevance and importance of the Post Office to our constitutional rights. Mr. Justice Holmes in United States ex rel. Milwaukee Social Democratic Pub. Co. v. Burleson, 255 U.S. 407, 437, 41 S.Ct. 352, 363, 65 L.Ed. 704 (dissenting opinion), said that 'the use of the mails is almost as much a part of free speech as the right to use our tongues.'

Id. at 251.
23. 90 F. Supp. 2d 263 (S.D.N.Y. 1999).

subsequent warrants. At trial, the defendant moved to suppress evidence obtained through the mail search.[24]

The court held that prisoners do not have an expectation of privacy with respect to searches performed by prison officials in order to maintain institutional security.[25] But even prisoners have a reasonable expectation of privacy regarding searches unrelated to institutional security that are conducted by law enforcement officers other than those in charge of the prison.[26]

Next, the court addressed the question of whether the mail search complied with the requirements of Federal Rule of Criminal Procedure 41(d), which generally mandates that officers executing a search warrant must provide contemporaneous notice to the person whose property was searched. The court concluded that the judge issuing a warrant can authorize a delay of seven days for giving notice.[27] Longer delays are permissible upon a strong showing of necessity. And additional delays can be granted upon subsequent application.[28] This aspect of the Rule gives law enforcement officers the latitude to conduct "sneak and peak" searches where contemporaneous notice would compromise the investigation.[29]

The court held that even though the nine-day period of time authorized by the initial warrant was two days too long, suppression of the evidence is not necessary unless "(1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule."[30] Neither of these circumstances was found to exist and so the motion to suppress was denied.[31]

Actually, Federal Rule of Criminal Procedure 41 made no mention of delayed notice at the time *Rollack* was decided.[32] Nevertheless, *Rollack* is consistent with several other federal decisions that create an exception to the statutory requirement of contemporaneous notice. These decisions provide an interesting foundation for the law of covert searches in general, though highly specialized rules govern the monitoring of telephone conversations and email messages.

---

24. *Id.* at 266–68.
25. *Id.* at 270.
26. *Id.* at 269–70. *But see* Willis v. Artuz, 301 F.3d 65 (2d Cir. 2002).
27. *Rollack*, 90 F. Supp. 2d at 271.
28. *Id.*
29. *Id.*
30. *Id.* (quoting United States v. Burke, 517 F.2d 377, 386–87 (2d Cir. 1975)).
31. *Id.* at 271–72.
32. FED. R. CRIM. PRO. 41 (1999).

B. *Other Covert Searches*

In *Dalia v. United States*,[33] the FBI installed an electronic bugging device in an office pursuant to judicial authorization issued according to the then-existing provisions of Title 18, Chapter 119.[34] The warrant did not expressly authorize the covert entry necessary to install the bug. The District Court denied the defendant's motion to suppress evidence of his monitored conversations,[35] and his conviction for receiving stolen goods was affirmed by the Third Circuit.[36]

On certiorari, the Supreme Court held that the Fourth Amendment does not absolutely prohibit law enforcement officers from making surreptitious entries associated with a judicially authorized search.[37] When covert activity is necessary, Fourth Amendment considerations are satisfied if the person who was subjected to surveillance is notified upon the conclusion of the operation.[38]

Nor does Fourth Amendment jurisprudence require prior, express judicial approval for a covert entry. The manner in which a search is executed is generally left to the discretion of law enforcement officers, subject only to the prohibition against "unreasonable searches and seizures."[39] Therefore, neither the covert entry nor the use of the eavesdropping device ran afoul of the Fourth Amendment. And the legislative history of 18 U.S.C. §§ 2510–22 reveals that Congress intended to permit covert entry when necessary to install the equipment needed for electronic surveillance.[40]

Dalia recognized the nexus between the privacy interests that are compromised by the "bugging" of private conversations in an office and

33. 441 U.S. 238 (1979).
34. 18 U.S.C. §§ 2510–2520 (1976).
35. United States v. Dalia, 426 F. Supp. 862 (D.N.J. 1977).
36. United States v. Dalia, 575 F.2d 1344 (3d Cir. 1978).
37. 441 U.S. 238, 247–48 (1979).
38. The Court wrote:

> It is well established that law officers constitutionally may break and enter to execute a search warrant where such entry is the only means by which the warrant effectively may be executed. . . . In United States v. Donovan, 429 U.S. 413, 429 n. 19 (1977), we held that Title III provided a constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance. *See* 18 U.S.C. § 2518(8)(d). There is no reason why the same notice is not equally sufficient with respect to electronic surveillances requiring covert entry. We make explicit, therefore, what has long been implicit in our decisions dealing with this subject: the Fourth Amendment does not prohibit *per se* a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment.

Dalia, 441 U.S. at 247–48 (emphasis in original).
39. *Id.* at 254–59.
40. *Id.* at 249–54.

the covert entry necessary to install the bugging equipment. Accordingly, the Court held that when Congress expressly authorized electronic surveillance with judicial approval, Congress implicitly authorized covert entry as may be necessary to install the electronic bug.[41]

While *Dalia* focused on narrow issues concerning electronic surveillance, *United States v. Freitas*[42] addressed the safeguards of Federal Rule of Criminal Procedure 41 governing execution of searches in general. *Freitas I* arose from an investigation of the manufacture of methamphetamine. At trial, the defendant moved to suppress evidence derived from a search of his home by DEA agents. The search was conducted pursuant to a warrant authorizing covert entry into a residence that was suspected of being used as a methamphetamine laboratory. The warrant permitted the DEA agents to enter the home without notice in order to look around while the residents were not present.[43]

The magistrate issued the warrant using a conventional form that was designed to comply with Federal Rule of Criminal Procedure 41.[44] However, he crossed off the item calling for a description of the property to be seized.[45] He also crossed off the boilerplate directing the FBI to leave a copy of the warrant at the residence along with an inventory of any property seized, so that the warrant did not contain any provision for notice to the residents.[46]

The District Court suppressed certain evidence, holding that surreptitious entry warrants are impermissible under the Constitution and also under Federal Rule of Criminal Procedure 41. Moreover, the "good faith" exception to the exclusionary rule did not make the evidence admissible. The Government appealed to the Ninth Circuit.[47]

There, the court held that the search violated the Fourth Amendment, but remanded the case to the district court for further findings of fact in order to determine whether the good faith exception took the evidence outside of the exclusionary rule.[48] The Ninth Circuit reasoned that the Fourth Amendment does not prohibit all covert entries.[49] However, the lack of an express provision in the warrant regarding service of notice rendered it constitutionally defective. The warrant could have survived a constitutional challenge by providing for notice within a reasonable time

41. *Id.* at 252.
42. 800 F.2d 1451 (9th Cir. 1986) [hereinafter *Freitas I*].
43. *Id.* at 1453.
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.* at 1453–54.
48. *Id.* at 1456–57.
49. *Id.* at 1456.

after the covert entry.[50] "Reasonable" was defined as not more than seven days except upon a strong showing of necessity.[51]

The Ninth Circuit also held that the surreptitious search did not comply with Federal Rule of Criminal Procedure 41, which provides inadequate guidance for judicial authorization of covert entries.[52] The court stated that the desirable amendments to the Rule should originate through legislative action rather than by way of judicial interpretation. The court resolved its uncertainty by concluding that the covert entry did not comply with the Rule. But such a lack of compliance does not require suppression of evidence unless law enforcement officers deliberately disregarded the Rule and would not have carried out the search if they had been forced to obey its terms. The district court was also instructed to make further findings of fact regarding this point.[53]

On remand, the district court again suppressed the evidence and the government again appealed to the Ninth Circuit. The Circuit Court held that the law enforcement officers acted in good faith and so the Fourth Amendment exclusionary rule need not be applied.[54] Nor did the statutory violation by law enforcement officers necessitate exclusion of the evidence in the absence of a clear constitutional violation or deliberate disregard of Rule 41.[55]

Freitas I contains an interesting comparison of the privacy interests that are compromised by surreptitious wiretapping and by covert entry into a person's residence. The court stated:

> The surreptitious character of the search and seizure in this case calls to mind wiretapping, which is now governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520 (1982) [also known as the Federal Wiretap Act]. The district court held that noncompliance both with Title III's notice provisions and with the "necessity for electronic surveillance requirement" existed in this case. Reasoning by analogy, the district court held the search and seizure violated the Fourth Amendment.

---

50. *Id.*

51. *Id.* at 1456–58.

52. *Id.* at 1456.

53. *Id.* at 1455–58.

54. United States v. Freitas, 856 F.2d 1425, 1428–32 (9th Cir. 1988) [hereinafter *Freitas II*].

55. *Id.* at 1432–33. *Freitas II* permitted the use of evidence held to have been obtained in violation of the Fourth Amendment and Rule 41 because the police acted in good faith. Later cases state that a search warrant requiring notice within a reasonable time after completion of a covert search complies with the requirements of the Fourth Amendment as well as Rule 41. *See* United States v. Johns, 948 F.2d 599, 603–06 (9th Cir. 1991); United States v. Villegas, 899 F.2d 1324, 1336–38 (2d Cir. 1990).

> Despite the similarity of the problems presented by this case and wiretapping, Title III has been held to apply only to *aural* interception of communication, *see New York Telephone Co.*, 434 U.S. at 166–67, 98 S. Ct. at 369–70, and not to *visual* observations. Title III, however, does serve to make clear the probable constitutional importance of both the necessity for the surreptitious seizure and the subsequent notice.
>
> With respect to a necessity requirement, the record before us fails to show that it was met. Perhaps it could have been, but, viewing the record as a whole, we conclude that it merely demonstrates that the search and seizure would facilitate the investigation of Freitas, not that it was necessary. We hasten to add, however, that we do not hold that a showing of necessity is constitutionally required in a case such as is before us. We merely wish to point out that any such showing is lacking here and that, had such a showing been made, it could have strengthened the claim that the search and seizure in this case met the commands of the Fourth Amendment.[56]

The reference to the requirement of "necessity" originates in *Berger v. New York*,[57] which will be discussed in detail at Section V.A., *infra. Berger* held in part that the Fourth Amendment requires police officers seeking authorization for a wiretap to demonstrate that the wiretap is necessary because alternatives are either impractical or dangerous. After *Berger,* the showing of necessity goes beyond the normal criteria for obtaining a standard search warrant,[58] because unlike a routine search, a wiretap can only be conducted surreptitiously without contemporaneous notice. Shortly after *Berger,* Congress codified this and other requirements in the Federal Wiretap Act.[59]

Freitas I made clear that it was not extending the "necessity" requirement of *Berger* to covert searches in general.[60] Yet the discussion

56. *Freitas I*, 800 F.2d at 1456. The Second Circuit has gone so far as to hold that law enforcement officers must make a showing of "reasonable necessity" to justify delay in providing contemporaneous notice when they wish to conduct a covert-entry search. However, the officers do not have to meet the same rigorous standards as set out in the Federal Wiretap Act. *Villegas*, 899 F.2d at 1337–38.

57. 388 U.S. 41 (1967).

58. Id. at 59–60.

59. See infra Part V.A.-B.

60. After the September 11, 2001 attacks on the World Trade Center and the Pentagon, Congress enacted the 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). Section 213 amended 18 U.S.C.A. § 3103a to authorize delayed notice of the execution of a search warrant if the court believes that contemporaneous notice would lead to an "adverse result," the warrant prohibits an actual seizure unless the court

reveals that the court saw a similarity between the privacy interests that are compromised by a covert wiretap and by a covert home search. Likewise, this similarity could be readily found with respect to a covert mail search or (as will be seen) the surreptitious monitoring of email.

Of course, it is impossible to quantify the extent to which various types of covert searches invade the privacy of the person under investigation.[61] But this article asserts that the same privacy interest is compromised by covert searches of letters in the mail, telephone wiretaps, and surreptitious monitoring of email. Moreover, the same privacy interest is compromised where law enforcement officers surreptitiously search a home or office to read letters, other paper documents, or even computer files stored there.

Regardless of the medium of communication and the manner in which the covert search is executed, the privacy protections should be the same when law enforcement officials covertly examine the expression of a person's private thoughts and ideas. Therefore, it would not be illogical to extend the procedural safeguards governing wiretapping to the covert search and seizure of "snail mail," email, and any documents that are stored in a person's home or office.[62]

---

believes that the seizure is justified by reasonable necessity, and the warrant requires that notice be given within a reasonable time. But the "adverse result" standard shifts the focus from the "necessity" standard that was discussed in *Freitas I*. The "necessity" standard addresses the extent to which alternatives other than the execution of a surreptitious search exist. *See* 18 U.S.C.A. § 2518(3) (Supp. 2003). The "adverse result" standard does not require consideration of less intrusive alternatives that might yield a similar result. Instead, it assumes that the search will be conducted, but merely requires consideration of the possibility that contemporaneous notice may lead to certain undesirable results that could be avoided if notice is delayed. Where 18 U.S.C.A. § 3103a (Supp. 2003) uses the phrase "reasonable necessity," it is only with regard to justification for a seizure during the execution of the search, but not a prerequisite that must be established in order to obtain authorization to conduct the covert search.

61. The Ninth Circuit theorized that:

> [S]urreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.

Freitas I, 800 F.2d at 1456. *But see* United States v. Pangburn, 983 F.2d 449, 454–55 (2d Cir. 1993) ("Indeed, it was our perception that a covert entry search for intangibles is less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. It is less intrusive than a wiretap or video camera surveillance because the physical search is of a relatively short duration, focuses the search specifically on the items listed in the warrant, and produces information as of a given moment. . . .") (citing United States v. Villegas, 899 F.2d 1324, 1337 (1990)).

62. *See* Paul V. Konovalov, Note, *On a Quest for Reason: A New Look at Surreptitious Search Warrants*, 48 HASTINGS L.J. 435, 472–73 (1997) (asserting that the federal statutory

Realistically, there is little chance that the entirety of wiretapping safeguards will be extended anytime soon. But this article will go on to argue for more uniform protections governing the surreptitious search and seizure of any media of communication deemed worthy of protection.

III. LIMITATIONS ON MAIL COVERS AND PEN REGISTERS IN THE ABSENCE OF FEDERAL FOURTH AMENDMENT PROTECTION

A. *The Law of Mail Covers*

It is clear that an ongoing police effort to covertly monitor the content of a person's mail or telephone conversations constitutes a serious invasion of privacy that is limited by the Fourth Amendment's prohibition of "unreasonable search and seizure." The same should be true of police efforts to monitor the content of email communications, though little case law exists in this area.[63]

Other surreptitious investigative techniques do not reveal the contents of communications, but arguably are so intrusive as to constitute a search for purposes of the Fourth Amendment. For example, postal employees conducting a "mail cover" will record information appearing on the outside of envelopes before making delivery to the addressee.[64] This information, which may include a return address or a postmark, could help the police to identify conspirators or to locate a fugitive.[65]

---

regulation of wiretapping could serve as a guide for issuance and execution of surreptitious search warrants in general).

63. *See* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996); *see, e.g.*, *infra* Part V.C.1.

64. Mail covers are extensively performed for law enforcement purposes, though they receive little attention. Elizabeth Amon & Michael Ravnitzky, *Mail-Watching Gains in Use: It's a Low-Tech Tool of Law Enforcement*, NAT'L L.J., April 1, 2000, at A1.

65. 1 LAFAVE, *supra* note 12, § 2.7(a), at 618. The current procedure authorizing a mail cover is set out at 39 C.F.R. § 233.3 (2003), which states in relevant part:

> (e) The Chief Postal Inspector, or his designee, may order mail covers under the following circumstances: . . .
>
> (2) When a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to:
>
> (i) Protect the national security,
>
> (ii) Locate a fugitive,
>
> (iii) Obtain information regarding the commission or attempted commission of a crime, or
>
> (iv) Assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.

LaFave argues that mail covers are objectionable because they reveal a person's continuing associations over time despite the fact that the contents of the letters are not read by law enforcement officials. According to LaFave, "it is the breadth of the intrusion rather than its depth at any particular instant in time which is most threatening to privacy."[66]

The Ninth Circuit disagreed with LaFave's analysis. In *United States v. Choate*,[67] the Postal Inspector in Charge, Los Angeles, authorized a thirty-day mail cover pursuant to the written request of a U.S. Bureau of Customs agent. Through the mail cover, federal agents learned of a bank where Choate maintained an account.[68] This information was necessary to support a charge of attempted tax evasion.[69]

The district court held that the mail cover was instituted in violation of postal regulations because the mail cover request merely stated in conclusory language that the defendant was suspected of smuggling large amounts of narcotics into the United States.[70] In contrast, 39 C.F.R. § 233.2(e)(1)(ii) required that the mail cover request set out reasonable grounds demonstrating that the mail cover would aid in locating a fugitive, or that it would assist in obtaining information about a crime or attempted crime.[71]

Moreover, the court held that the mail cover constituted a warrantless search.[72] The court explained that a reasonable person realizes that the return address on a letter is necessary to route it back to the sender in the event of a problem with the name or address of the intended recipient. But a reasonable person would expect the return address to be used only for postal purposes and that no records would be maintained. Because the mail cover violated a reasonable expectation of privacy without judicial authorization, evidence derived from it was suppressed.[73]

On appeal of the suppression order, the Ninth Circuit held that the mail cover complied with the applicable postal regulations.[74] The court explained that the conclusions expressed in the mail cover request were sufficient to satisfy the regulations without spelling out the underlying facts in support of those conclusions.[75]

66. 1 LAFAVE, *supra* note 12, § 2.7, at 618.
67. 422 F. Supp. 261 (C.D. Cal. 1976), *rev'd* 576 F.2d 165 (9th Cir. 1978).
68. *Choate*, 422 F. Supp. at 268 n. 12.
69. *Id.* at 263.
70. *Id.* at 264–67.
71. *Id*. at 263–67 (applying 38 C.F.R. § 233.2(e)(1)(ii) (1975)).
72. *Id.* at 271.
73. *Id.* at 267-71.
74. *Choate*, 576 F.2d at 171–73.
75. *Id.*

The mail cover did not amount to a search because information appearing on the outside of an envelope is readily available to be seen by postal employees. And since it is the sender who exposed the information to view, the recipient can have no privacy interest where he does not have the ability to prevent the information from being seen.[76] Therefore, the order granting the motion to suppress evidence was reversed.[77]

B. *The Law of Pen Registers*

A pen register is a device that can be attached to a telephone line, usually at a central telephone company office, for the purpose of covertly recording outgoing telephone numbers dialed. The pen register does not indicate whether anyone answers the outgoing call. The pen register will also detect and record the number of times a telephone rings when incoming calls are received, but does not identify the phone number where the call originated. Nor does it reveal whether the incoming call is answered. Pen registers neither monitor nor record the content of telephone conversations.[78] As distinguished from a pen register, a trap and trace device performs a function akin to caller ID by recording the telephone number of incoming calls.[79]

In *United States v. New York Telephone Co.*,[80] the Supreme Court held that the use of pen registers was not governed by the Federal Wiretap Act, which at that time prohibited the interception of oral or wire communication except in accordance with its provisions.[81] Because pen registers do not acquire the contents of telephone conversations, they do not "intercept" a communication as defined by the statute. Moreover, the legislative history of the Federal Wiretap Act shows that there was no intent to regulate the use of pen registers.[82]

The Supreme Court went on to affirm the power of the federal District Court to authorize installation of a pen register based upon a showing of probable cause. But the Supreme Court pointed out that all parties agreed that probable cause existed, and so it was unnecessary to

76. *Id.* at 174–78.

77. *Id.* at 183.

78. 1 LAFAVE, *supra* note 12, § 2.7(b), at 622 (citing United States v. Caplan, 255 F. Supp. 805 (E.D. Mich. 1966)).

79. David L. Sobel, *Privacy and Law Enforcement in the Digital Age*, 18 COMM. LAW. 3, 4 n.9 (Winter 2000).

80. 434 U.S. 159, 165–68 (1977).

81. The Federal Wiretap Act was subsequently amended by the Electronic Communications Privacy Act to also govern the interception of electronic communications. *See infra* Part V.B.3.

82. 434 U.S. at 165–68.

consider whether pen register installation was subject to the requirements of the Fourth Amendment.[83]

In *Smith v. Maryland*,[84] the Supreme Court held that use of a pen register does not amount to a search for purposes of the Fourth Amendment because a person cannot claim a reasonable expectation of privacy in information that he has turned over to a third party. More specifically, a caller has no reasonable expectation of privacy in the number he dials because that number must be conveyed to the telephone company in order to complete the call. Moreover, it is common knowledge that the telephone company has the ability to make permanent records of each call because toll calls are itemized on monthly billing statements. By making a telephone call, the caller runs the risk that the telephone company will reveal the phone number to the police.[85]

And even though the phone company typically does not itemize local calls on a monthly billing statement, no reasonable expectation of privacy exists for local phone numbers dialed because the phone company could elect to itemize those numbers as well. The fact that the phone company may choose not to itemize local calls in its monthly statements to subscribers does not create a reasonable expectation of privacy in those numbers. Once a phone number is voluntarily conveyed to the phone company, that number can be divulged to law enforcement officers regardless of whether current billing policy actually provides for itemization in a printed billing statement.[86]

The outcome of these two decisions left the installation of pen registers unrestricted by federal statute or the Fourth Amendment until the Electronic Communications Privacy Act (ECPA)[87] was enacted in 1986.[88] The ECPA expressly regulated the use of pen registers and also updated the Federal Wiretap Act. As codified at 18 U.S.C. § 3121 and amended, the statute states that: "(a) In general. Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or

83. *Id.* at 168–69.
84. 442 U.S. 735 (1979).
85. *Id.* at 742–46.
86. *Id.*
87. Pub. L. No. 99-508, 100 Stat. 1848 (1986).
88. LaFave asserts that "under *Smith*, the police may without any cause whatsoever and for whatever purpose they choose uncover private relationships with impunity." 1 LAFAVE, *supra* note 12, § 2.7(b), at 626. Despite the absence of federal judicial oversight, it had been held that pursuant to the Colorado Constitution, use of a pen register constitutes a search and seizure requiring a warrant based on probable cause in the absence of exigent circumstances or consent. People v. Sporleder, 666 P.2d 135, 144 (Colo. 1983).

under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §§ 1801–63).[89]

18 U.S.C. § 3123(a)(1)–(2) authorizes 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 certifying only "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[90] The order approving the installation must include, *inter alia*, the identity, if known, of the person under investigation, and a statement of the offense under investigation.[91]

The operation of the pen register or trap and trace device shall not exceed 60 days,[92] but the court can grant an extension for an additional 60 days upon another showing that information likely to be obtained will continue to be relevant to the investigation.[93] The court can order the provider of wire or electronic communication service to lend technical support to law enforcement officers as necessary to set up the pen register or trap and trace device.[94] Further, the court can prohibit them from revealing the existence of the investigation.[95]

In limited emergency situations, certain designated officials can order the installation of a pen register or trap and trace device before judicial authorization is obtained.[96] But such use must terminate within 48 hours unless judicial approval is obtained.[97]

18 U.S.C. § 3121(d) states that a knowing violation of the general prohibition against use of pen registers or trap and trace devices is punishable by fines and imprisonment for up to one year.[98] Significantly, the statute does not mandate the exclusion of evidence obtained in violation of its prohibitions. The lack of an exclusionary rule is not surprising since the use of a pen register does not constitute a search for

89. The USA PATRIOT Act, section 216, amended 18 U.S.C. § 3127 to expand the definition of pen register to include software as well as a mechanical device that records outgoing telephone numbers. Moreover, the definition was broadened to make clear that the statute governs efforts to obtain equivalent information such as the destination address for email and other types of electronic communication.

Likewise, the definition of trap and trace device was expanded to include software that records the telephone number from which an incoming call originated. And the definition was broadened to make clear that the statute also governs efforts to obtain equivalent information such as the originating address for email and other types of electronic communication.

90. 18 U.S.C.A. §§ 3123(a)(1)–(2) (Supp. 2003). This certification is far less than the showing of probable cause necessary to support an application for a standard search warrant.

91. *Id.* § 3123(b)(1).

92. *Id.* § 3123(c)(1).

93. *Id.* § 3123(c)(2).

94. *Id.* § 3123(b)(2).

95. *Id.* § 3123(d).

96. *Id.* § 3125(a).

97. *Id.* § 3125(b).

98. *Id.* § 3121(d).

purposes of the Fourth Amendment. And the courts have been unwilling to create an exclusionary remedy that is not expressly called for by the language of the statute.[99]

It is possible that the functionality of the traditional pen register will expand in the foreseeable future, requiring further judicial oversight as the technology becomes more intrusive. Such increased capabilities have already been mandated by Federal Communications Commission regulations promulgated pursuant to the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[100] However, the relevant part of those regulations has been vacated by the D.C. Circuit.[101]

CALEA was enacted due to concern that advances in telecommunications technology are making it increasingly difficult for law enforcement agencies to conduct wiretaps and similar activities. For example, copper cables and traditional switches are being replaced with fiber optic lines and computers. Cellular phones that are not tied to a fixed location have become commonplace. In response to these technological innovations, CALEA was intended to clarify the duty of the telecommunications industry to cooperate with law enforcement agencies.[102]

The four general requirements imposed by 47 U.S.C. § 1002(a) upon the telecommunications industry can be summarized as follows:

> Telecommunications carriers are to be capable of: (1) quickly obtaining, for government use, specific communications pursuant to a court order; (2) quickly allowing the government access to "call-identifying information that is reasonably available;" (3) delivering the intercepted communications and call-identifying information to the government over equipment provided by the carrier for the government; and (4) providing the previous functions without interference to telecommunication services and preventing unauthorized interceptions.[103]

For purposes of the current discussion, it is the ability to access call-identifying information that is relevant to the use of pen registers. Call-identifying information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each

99. *See* United States v. Thompson, 936 F.2d 1249, 1251–52 (11th Cir. 1991).

100. Pub. L. No. 103-414, 108 Stat. 4279 (1994).

101. *See* U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450, 460–63 (D.C. Cir. 2000).

102. Michael A. Rosow, Note, *Is "Big Brother" Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies to Use Dialed Digital Extraction*, 84 MINN. L. REV. 1051, 1058–60 (2000).

103. *Id.* at 1061 (summarizing 47 U.S.C. § 1002(a) (1994).

communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[104]

47 U.S.C. § 1006 goes on to encourage the telecommunications industry to establish standards for compliance with the requirements of CALEA. Carriers who abide by these standards qualify for a "safe harbor" to avoid fines for failure to meet the statutory requirements.[105] If the industry fails to adopt a set of standards, or if a Government agency or other interested person believes those standards are deficient, the agency or person can petition the Federal Communications Commission to establish its own regulations.[106]

After two years of proceedings and negotiations between the Telecommunications Industry Association (TIA) and the FBI, the TIA published its technical standards in accordance with the safe harbor provisions of CALEA. These standards were challenged as deficient by the Center for Democracy and Technology, the Justice Department, and the FBI. In response to this challenge, the FCC ultimately promulgated regulations.[107]

The regulations, in relevant part, require telecommunications carriers to provide "post-cut-through dialed digit extraction" to law enforcement officials pursuant to a pen register warrant.[108] Post-cut-through dialed digit extraction may be explained as follows:

> This . . . capability requires carriers to monitor electronically the communications channel that carries audible call content in order to decode all digits dialed after calls are connected or "cut through." Some post-cut-through dialed digits are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. Post-cut-through dialed digits can also represent call content. For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And

104. 47 U.S.C. § 1001(2) (1994).
105. *Id.* § 1006(a)(2).
106. *Id.* § 1006(b).
107. 14 F.C.C.R. 16794 (1999), 47 C.F.R. §§ 22.1103, 24.903, 64.2203 (1999). See Rosow, *supra* note 102, at 1063–65, *and* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454–57 (2000), for a summary of the process leading up to the drafting of these regulations.
108. In the Matter of Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, 16846 ¶ 123 (1999).

when calling pharmacies to renew prescriptions, they enter prescription numbers.[109]

The FCC regulations requiring post-cut-though dialed digit extraction were challenged in federal court and vacated by *United States Telecom Ass'n v. Federal Communications Commission*.[110] The D.C. Circuit correctly recognized that some digits dialed after the call has been completed may constitute content rather than mere call-identifying information.[111]

The court hypothesized that a full-blown wiretap warrant might be required in order to authorize law enforcement officials to obtain any digits dialed after the call is completed.[112] Yet the FCC regulations require the telecommunications carrier to turn over all dialed digits based on a pen register warrant even though current technology is unable to distinguish between "digits dialed to route calls and those dialed to communicate information."[113] Therefore, this aspect of the agency's order was vacated for failure to "protect the privacy and security of communications not authorized to be intercepted."[114]

The FCC regulations constitute a clear example of a technology-driven approach to electronic eavesdropping. In drafting its regulations, the FCC wrongly focused on the technology rather than on the nature of the privacy interests at risk. The agency regulations seemed to assume that technology designed to record digits is simply a pen register even if those digits constitute call content rather than "call-identifying information." Fortunately, the D.C. Circuit looked beyond the technology and recognized the extent of the intrusion upon privacy interests. When the intrusion amounts to a wiretap, nothing short of a wiretap warrant can authorize such activity.[115]

---

109. *U.S. Telecom Ass'n*, 227 F.3d at 462.

110. *Id.* at 463. The United States Telecom Association and the Cellular Telecommunications Industry Association, joined by the Center for Democracy and Technology, filed a petition for review of the FCC regulations. Petitions were also filed by the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the American Civil Liberties Union. *Id.* at 456–57.

111. *Id.* at 462.

112. *Id.*

113. *Id.*

114. *Id.* at 462–63.

115. In response to the decision of the D.C. Circuit, the FCC issued new regulations that again require telephone companies to have the capability to provide post-cut-through dialed digit extraction. But the new regulations make clear that post-cut-through digits are to be provided to a law enforcement agency only pursuant to the appropriate judicial authorization. Thus, the new regulations carefully avoid any attempt to determine the legal standard under which the information must be made available to a law enforcement agency. This issue is correctly left entirely to the courts. In the Matter of Communications Assistance for Law Enforcement Act, 17 F.C.C.R. 6896 ¶¶ 66–93 (2002).

IV. HISTORICAL OVERVIEW OF THE EARLY LAW GOVERNING WIRETAPS

A. *The Supreme Court Initially Provides Little Protection Against Wiretapping in the Absence of Federal Statute*

Any history of the law governing wiretaps should include a discussion of *United States v. Olmstead*,[116] which is significant for its narrow view of a person's constitutionally protected privacy interests. It seems that prohibition agents suspected Olmstead and his attorney, Finch, of conspiring to violate the National Prohibition Act. Without obtaining a search warrant, the prohibition agents wiretapped the telephones of Olmstead and Finch and overheard incriminating discussions.

At trial, the District Court permitted the prosecution to introduce evidence of the telephone conversations. In reaching this conclusion, the court discussed the issue of attorney-client privilege, but did not address the issue of search and seizure. The court held that Olmstead and Finch, as participants in an ongoing conspiracy, could not properly claim that their conversations were privileged.[117] Even if their conversations qualified for the protection of attorney client privilege, the privilege was lost for failure to prevent others from discovering what was said. The court reasoned that "[a] third person is not forbidden to relate a confidential conversation heard by him. Wire tapping is not a national offense, nor made so by the statutes of the state of Washington; even so, it would not violate any constitutional right of the defendants to receive the testimony."[118]

On appeal of Olmstead's conviction, the Ninth Circuit agreed that evidence derived from the wiretaps was admissible. The court held that:

> The protection of [the Fourth and Fifth] amendments, however, has never been extended to the exclusion of evidence obtained by listening to the conversation of persons at any place or under any circumstances. The purpose of the amendments is to prevent the invasion of homes and offices and the seizure of incriminating

116. 7 F.2d 760 (W.D. Wash. 1925), *aff'd*, 19 F.2d 842 (9th Cir. 1927), *aff'd*, 277 U.S. 438 (1928).

117. 7 F.2d at 763.

118. *Id.* This holding reflected the prevailing view of the attorney client privilege at the time. The court further illustrated its point as follows:

> If the conversation referred to had been carried on in the home of the defendant Olmstead, between him and his attorney, and the conversation had been heard by trespassers on the premises, it would be competent testimony in support of the criminal charge. I know of no rule of law or evidence which would exclude it. . . .

Id.

> evidence found therein. Whatever may be said of the tapping of telephone wires as an unethical intrusion upon the privacy of persons who are suspected of crime, it is not an act which comes within the letter of the prohibition of constitutional provisions.[119]

The dissent by Judge Rudkin includes an interesting comparison of the privacy interests associated with letters in the mail and telephone conversations. He rejected the analysis that simply looked to whether a trespass took place when the information was acquired by law enforcement officials. Judge Rudkin realized that the court should look to the privacy interests at stake in order to decide whether a search warrant is required before law enforcement officers covertly intrude on the private exchange of ideas between two parties. Judge Rudkin explained:

> In discussing the protection that surrounds a letter deposited in the mail, in Ex parte Jackson, 96 U.S. 727, 733 (24 L. Ed. 877), Mr. Justice Field said:
>
> "Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the Fourth Amendment of the Constitution."
>
> And it is the contents of the letter, not the mere paper, that is thus protected. What is the distinction between a message sent by letter and a message sent by telegraph or by telephone? True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference. A person using the telegraph or telephone is not broadcasting to the world. His

119. 19 F.2d at 847.

> conversation is sealed from the public as completely as the nature of the instrumentalities employed will permit, and no federal officer or federal agent has a right to take his message from the wires, in order that it may be used against him. Such a situation would be deplorable and intolerable, to say the least. Must the millions of people who use the telephone every day for lawful purposes have their messages interrupted and intercepted in this way? Must their personal, private, and confidential communications to family, friends, and business associates pass through any such scrutiny on the part of agents, in whose selection they have no choice, and for the faithful performance of whose duties they have no security? Agents, whose very names and official stations are in many instances concealed and kept from them. If ills such as these must be borne, our forefathers signally failed in their desire to ordain and establish a government to secure the blessings of liberty to themselves and their posterity.[120]

After the Ninth Circuit affirmed the district court, the U.S. Supreme Court accepted the case on certiorari.[121] In a 5-4 decision, the Court held that the wiretaps were not subject to restrictions imposed by the Fourth or Fifth Amendments. In reaching this conclusion, the Court observed that the police set up the wiretaps in the basement of a large office building and in the street near the homes of some of the defendants.[122] Significantly, the police implemented all of the wiretaps without entry into the defendants' offices or houses. The Court reasoned that the protections of the Fourth Amendment cannot be expanded to include telephone wires "reaching to the whole world from the defendant's house or office."[123]

Rather, the Court concluded that the Fourth Amendment is not violated as against a defendant "unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[124] According to this narrow view of the Fourth Amendment, there was no search or seizure where the police used only their sense of hearing and did not enter the house or office of any of the defendants.[125] The Court explained that Congress could "protect the

120. *Id.* at 849–50 (Rudkin, J., dissenting).

121. Olmstead v. United States, 276 U.S. 609 (1927). The Court agreed to consider only whether the wiretaps violated the Fourth and Fifth Amendments.

122. 277 U.S. 438, at 456–57 (1928).

123. *Id.* at 465.

124. *Id.* at 466.

125. *Id.* at 464.

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."[126]

In his dissent, Justice Brandeis argued that the Constitution should be interpreted broadly so that its protections against governmental abuses of power can be adapted to a changing world.[127] His famous dissent asserted that:

> [The 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. To protect that right, 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.[128]

Apart from the constitutional issues of search and seizure, Justice Brandeis believed that the wiretap evidence was inadmissible because it was obtained in violation of state statute. He eloquently argued that:

> Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means—to declare that the government may commit crimes in order to secure the conviction of a private criminal—would

126. *Id.* at 465–66. The Court distinguished the protection for letters in the mail as set out by *Ex parte Jackson* on the basis that the Fourth Amendment safeguards tangible letters in the care of a government sanctioned monopoly. However, Fourth Amendment protection does not extend to intangible conversations carried over the telephone lines. *Id.* at 464. Moreover, the Court was unconcerned about the existence of a Washington state statute that prohibited the interception of messages transmitted via telephone lines. That statute did not expressly mandate that evidence of intercepted messages is inadmissible in court. Even if the statute had explicitly done so, state law could not govern the admissibility of evidence in federal court. Additionally, evidence is not inadmissible at common law even when it was obtained illegally. *Id.* at 466–69. And the wiretap did not violate the Fifth Amendment in the absence of any compulsion to induce the defendants to talk on the telephone. *Id.* at 462.

127. *Id.* at 472–74 (Brandeis, J., dissenting).

128. *Id.* at 478.

> bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.[129]

B. *Early Federal Statutory Limitations on Wiretaps*

As originally enacted, section 605 of the Federal Communications Act of 1934 (hereinafter "section 605") stated:

> No person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee. . . No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . .[130]

Before long, the Supreme Court had an opportunity to begin interpreting the statute. In *Nardone v. United States*,[131] the defendants were convicted in federal district court of illegally possessing, concealing, and smuggling alcohol, as well as related conspiracy offenses. Having conducted wiretaps, federal agents testified in court as to the substance of the defendant's interstate telephone conversations.

The Supreme Court reversed the conviction on the basis that:

> Section 605 of the Federal Communications Act provides that no person who, as an employee, has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employees, save in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . .[132]

The Court concluded:

---

129. *Id.* at 485.

130. Federal Communications Act of 1934, ch. 652, Title VI § 605, 48 Stat. 1064, 1103–04 (1934) (current version at 47 U.S.C. § 605 (2000)).

131. 302 U.S. 379 (1937).

132. *Id.* at 380–81.

> [T]he plain words of [section] 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that "*no person*" shall divulge or publish the message or its substance to "*any person*." To recite the contents of the message in testimony before a court is to divulge the message. The conclusion that the act forbids such testimony seems to us unshaken by the government's arguments.[133]

While *Nardone* held that evidence of illegally wiretapped interstate telephone calls was inadmissible in federal court, *Weiss v. United States*[134] went a step further in holding that section 605 also banned the wiretapping of intrastate telephone calls. Accordingly, evidence obtained through an illegal wiretap of an intrastate phone call was likewise inadmissible in federal court.[135] And in *Benanti v. United States*,[136] the Supreme Court held that section 605 required the exclusion of wiretap evidence in federal court even though state law enforcement officers conducted the wiretap pursuant to a search warrant that was properly issued under state law.[137]

However, section 605 did not entirely preclude consideration of wiretap evidence in federal court. For example, a person who did not participate in a wiretapped conversation lacked standing to object to the admissibility of evidence obtained through the wiretap.[138] If a participant consented to a wiretap, evidence of the conversation was admissible as against the other party to the conversation even though that person was unaware of the wiretap.[139]

The Supreme Court held in *Schwartz v. Texas* that section 605 was not applicable to the states, so that state law determined whether wiretap evidence was admissible in state court.[140] Thus, the Texas Court of Criminal Appeals held in 1953 that a telephone operator who eavesdropped on a conversation between an attorney and his client could testify at trial where the client was accused of murdering his ex-wife.[141] It

133. *Id.* at 382.
134. 308 U.S. 321 (1939).
135. *Id.* at 326–31.
136. 355 U.S. 96 (1957).
137. *Id.* at 104–05.
138. Goldstein v. United States, 316 U.S. 114, 121 (1942).
139. Rathbun v. United States, 355 U.S. 107, 110–11 (1957).
140. 344 U.S. 199, 203 (1952).
141. Clark v. State, 261 S.W.2d 339, 347 (Tex. Crim. App. 1953). At the time, state law did not exclude evidence that was obtained by eavesdropping. Although Texas courts recognized the attorney client privilege, the attorney and client were held responsible to ensure that their conversations were not overheard. If an eavesdropper succeeded in overhearing a confidential conversation between attorney and client, that eavesdropper could testify in court as to what was said. *Id.* at 342. Even though the telephone operator violated telephone company

was not until 1968 that the Supreme Court expressly overruled *Schwartz*, holding that section 605 was applicable to the states.[142]

In spite of the plain language of section 605, federal authorities conducted wiretaps in furtherance of foreign intelligence activities, arguing that such activities were not entirely prohibited. The Department of Justice and the FBI also engaged in wiretapping associated with investigations of domestic crimes on the theory that section 605 did not proscribe wiretapping per se, but prohibited wiretapping followed by "divulgence." They took the position that there was no divulgence for purposes of section 605 when a governmental official passed the information on to another.[143]

V. MODERN CONSTITUTIONAL AND STATUTORY PROTECTIONS FOR WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS

A. *Modern Fourth Amendment Limitations on Telephone Wiretaps*

Section 605 governed the admissibility of wiretap evidence in federal court. But other forms of electronic eavesdropping fell outside the scope of the statute. Under the rationale of *Olmstead*, these alternative forms of eavesdropping did not amount to a search for Fourth Amendment purposes in the absence of a physical trespass. As a result, new electronic eavesdropping technologies went essentially unregulated.[144]

For example, *Goldman v. United States*[145] held that evidence obtained by federal law enforcement officers was admissible where the officers were lawfully present in an office and placed a "detectaphone" against a wall in order to overhear a conversation in the next room.[146] *On Lee v. United States*[147] held that evidence acquired by federal agents was admissible where they hid a microphone on a person who entered the defendant's home with his consent.[148]

---

policy by eavesdropping on a telephone conversation, her testimony was admissible and the defendant was sentenced to death. This case demonstrates that as recently as the 1950s, use of the telephone for sensitive communications could be a dangerous practice.

142. Lee v. Florida, 392 U.S. 378, 385 (1968). Ultimately, Lee had little impact because it was decided just two days before enactment of the Federal Wiretap Act of 1968, discussed *infra* at Part VB, which provided new regulation of electronic eavesdropping. 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 2d ed. § 4.1(b), at 329–30 (2d ed. 1999).

143. 2 LAFAVE ET AL, *supra* note 142, § 4.1(b), at 328–29.

144. *Id.* § 4.1(c), at 330.

145. 316 U.S. 129 (1942).

146. *Id.* at 131–33.

147. 343 U.S. 747 (1952).

148. *Id.* at 751–58.

But the Supreme Court began to take a more expansive view of the Fourth Amendment during the 1960s. In *Silverman v. United States*,[149] the police placed a "spike mike" (a microphone with a spike attached to it, along with an amplifier, power pack, and earphones) into the common wall of a row house until it made contact with a heating duct. The spike mike enabled the police to overhear the conversations of the occupants of the adjacent house.[150] The Supreme Court held that evidence of the conversations was inadmissible without consideration of whether the police had committed a technical trespass under local property law.[151] Subsequently, *Wong Sun v. United States*[152] expressly recognized that the Fourth Amendment offers protection against police efforts to overhear conversations as well as protection against the seizure of tangible items.[153]

In 1967, the Supreme Court established the presently accepted standard for Fourth Amendment protection in *Katz v. United States*.[154] There, the FBI attached an electronic device to the exterior of a telephone booth in order to monitor and record the defendant's side of several telephone conversations concerning illegal gambling activities.[155] The Court held that tape recordings of the conversations were inadmissible in evidence because:

> [T]he underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.[156]

Katz made clear that that the Fourth Amendment places limits on the implementation of technology for purposes of eavesdropping by law enforcement officers in the absence of consent by one of the parties to the

149. 365 U.S. 505 (1961).
150. *Id.* at 506–07.
151. *Id.* at 511–12.
152. 371 U.S. 471 (1963).
153. *Id.* at 485.
154. 389 U.S. 347 (1967).
155. *Id.* at 348.
156. *Id.* at 353. Justice Harlan's concurring opinion explained that Fourth Amendment protections are invoked when "a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' " *Id.* at 361.

conversation.[157] The extent of these limits as applied to telephone wiretapping was spelled out in great detail by *Berger v. New York*.[158]

Berger addressed the constitutionality of a New York statute setting out an *ex parte* procedure for judicial authorization of electronic eavesdropping. The statute was found to be in violation of the Fourth and Fourteenth Amendments for several reasons. First, the statute did not require the search warrant to sufficiently describe the crime under investigation, nor "the place to be searched" nor "the persons or things to be seized".[159] Second, the statute did not require a sufficiently "precise and discriminate" description of the conversations that the police wanted to monitor.[160] Third, the statute authorized eavesdropping for an extended period of time that was deemed to violate the requirement of prompt execution.[161] Fourth, the statute permitted extension of the time period without sufficient showing of probable cause for the continuation.[162] Fifth, the statute did not require termination of the eavesdropping when the police overheard the conversation they were waiting for.[163] Sixth, 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.[164] Lastly, the statute lacked any provision for a return of service on the warrant to account for the records of conversations that had been overheard.[165]

B. *Modern Federal Statutory Limitations on Telephone Wiretaps and Interception of Email*

1. The Omnibus Crime Control and Safe Streets Act of 1968 Amends Section 605

By the time of *Katz* and *Berger*, it was generally agreed that the prohibition against interception and divulgence of telephone conversations as mandated by section 605 needed to be reassessed.[166] Accordingly, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Federal Wiretap Act)[167] was enacted at 18 U.S.C. §§ 2510–20 in order to strike a

157. 2 LAFAVE ET AL, *supra* note 142, § 4.1(c), at 331.
158. 388 U.S. 41 (1967).
159. *Id.* at 55–56.
160. *Id.* at 56–59.
161. *Id*. at 59.
162. *Id.* at 59.
163. *Id.* at 59–60.
164. *Id.* at 60.
165. *Id.*
166. 2 LAFAVE ET AL., *supra* note 142, § 4.2(a), at 332.
167. Pub. L. No. 90-351, 82 Stat. 197 (codified at 18 U.S.C. §§ 2510–2520 (Supp. V 1965–1969)).

new balance between the right to privacy and the needs of law enforcement. Section 605 was amended to create exceptions to its prohibition against interception and divulgence of wire communications.[168] Thus, the statutory regulation of wiretaps shifted from section 605 to the Federal Wiretap Act.

According to the new provisions, the willful interception of oral or wire communication was prohibited except as permitted therein. Section 2511 as originally enacted stated:

> Except as otherwise specifically provided in this chapter any person who—
>
> (a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;
>
> . . .
>
> (c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection;
>
> . . .
>
> shall be fined not more than $10,000 or imprisoned not more than five years, or both.[169]

Section 2510 defined wire and oral communications as follows:

> As used in this chapter—
>
> (1) "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;
>
> (2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such

168. Pub. L. No. 90-351, § 803, 82 Stat. 197, 223.
169. 18 U.S.C. § 2511 (Supp. V 1965–1969).

> communication is not subject to interception under circumstances justifying such expectation.[170]

Section 2515 of the Federal Wiretap Act added an exclusionary rule stating:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial . . . before any court . . . of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.[171]

The Federal Wiretap Act spells out the criteria that must be established before a court can authorize the interception of a wire or oral communication by law enforcement officials. To ensure compliance with the holding of *Berger*, these criteria go beyond the showing necessary to obtain a search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 3103a.

As originally enacted, section 2516(1) empowered the Attorney General, Deputy Attorney General, and certain other officials to ask a federal judge for authorization to intercept wire or oral communications pursuant to an investigation of specifically enumerated crimes. The interception was to be accomplished by a federal agency with responsibility for investigating the offense that was thought to have been committed.[172]

Similarly, section 2516(2) granted authority in conformance with federal as well as state law for the principal prosecutor of any state or county to ask a state judge for permission to intercept wire or oral communications. Once again, the federal statute required the interception to be accomplished by the appropriate law enforcement agency, and limited the interception to instances where it may provide evidence of certain specific crimes.[173]

A judge can issue an interception order only in accordance with section 2518, whose provisions are summarized by LaFave, Israel, and King as follows:

> 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

170. *Id.* § 2510.
171. *Id.* § 2515.
172. *Id.* § 2516(1).
173. *Id.* § 2516(2).

> 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.[174]

The Federal Wiretap Act permits interception before obtaining judicial authorization in emergencies. But the interception must terminate within 48 hours or as soon as the communication sought is obtained unless further interception is approved by a judge.[175] The Act mandates the judge to ensure that the target of the interception is served with an inventory providing notice of the interception within 90 days after completion of the surveillance.[176]

The Federal Wiretap Act originally contained language indicating that its provisions did not limit the constitutional power of the president to deal with matters such as foreign intelligence and national security.[177] This provision was repealed upon enactment of the Foreign Intelligence Surveillance Act of 1978.[178]

---

174. 2 LAFAVE ET AL., *supra* note 142, § 4.2(a), at 333.
175. 18 U.S.C. § 2518(7) (2000).
176. 18 U.S.C. § 2518(8)(d).
177. 18 U.S.C. § 2511(3) (Supp. V 1965–1969).
178. 2 LAFAVE ET AL., *supra* note 142, § 4.3(d), at 362–63.

2. Early Difficulties in Applying the Federal Wiretap Act to New Telephone Technologies such as Mobile Telephones and Cordless Telephones

Of course, the Federal Wiretap Act went into force before cellular telephones[179] and cordless telephones[180] became widely accepted. Although mobile telephones[181] (the predecessor of cellular phones) had existed for many years, they were not in widespread use. But it was not long before the Federal Wiretap Act's definitions of "oral communication" and "wire communication" led the courts to struggle with the interpretation of the statute in light of new telephone technologies.

For example, *U.S. v. Hall* involved defendants who conducted conversations over mobile telephones that were installed in two cars.[182] Some of their conversations were overheard by a private individual using a common eight-band radio that was readily available for purchase by the general public.[183]

The eavesdropper considered the conversations to be suspicious and continued to listen in for about a month before notifying the police, who began to monitor further conversations without judicial authorization.[184] The defendants were eventually arrested by state law enforcement

---

179. Senate Report No. 99-541 regarding the Electronic Communications Privacy Act of 1986 briefly explains cellular technology as follows:

> In a cellular radiotelephone system, large service areas are divided into honeycomb-shaped segments or "cells"—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone, typically in a motor vehicle, moves from cell to cell.

S. REP. NO. 99-541, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3563.

180. A cordless telephone consists of a hand-held mobile unit and a base unit. The speaker's voice is converted into radio waves and travels from the mobile unit to the base unit. The base unit in turn transmits the speaker's voice to the receiving party through ordinary telephone lines. Conversely, the incoming caller's voice is transmitted through the phone lines to the base unit, from which it travels to the mobile unit via radio waves. State v. Delaurier, 488 A.2d 688, 690 (R.I. 1985).

181. As early as 1949, the Federal Communications Commission allocated a small number of frequencies for mobile phones. Rather than employing multiple cells that each contain a transmitter, an individual transmitter served a 75 square mile area. Often, a single transmitter served an entire city. Therefore, the mobile phone industry was quite restricted. *See* Timothy R. Rabel, Comment, *The Electronic Communications Privacy Act: Discriminatory Treatment for Similar Technology, Cutting the Cord of Privacy*, 23 J. MARSHALL L. REV. 661, 662 (1990).

182. 488 F.2d 193 (9th Cir. 1973).

183. *Id.* at 194–95.

184. *Id.* at 195.

officers and turned over to federal authorities for prosecution. They were convicted of possession of marijuana with the intent to distribute it. The defendants appealed to the Ninth Circuit, arguing that evidence of their telephone conversations should have been suppressed.[185]

The Ninth Circuit had to decide whether a conversation over a mobile phone should be viewed as a wire communication that must be suppressed at trial, or an oral communication that need be suppressed only if the participants had a reasonable expectation that their conversation was not subject to interception.[186] This decision was complicated by the lack of guidance in the legislative history of the Federal Wiretap Act.[187]

The court interpreted the statute to require that when one side of a conversation takes place over a wire telephone and the other side utilizes a mobile telephone, the conversation must be treated as a wire communication that should be suppressed in the absence of judicial authorization to conduct a wiretap.[188] In contrast, a conversation taking place over two mobile telephones would be treated as an oral communication that need be suppressed only if the parties reasonably believed that their conversation would not be intercepted.[189] The case was remanded to the district court for further findings as to whether certain conversations should be regarded as "oral" or "wire," and whether the parties to any oral communication had a reasonable expectation of privacy.[190]

A federal district court came to a different conclusion under similar circumstances in *Edwards v. Bardwell*.[191] There, Edwards used the mobile phone in his car to contact his attorney on the attorney's wire telephone. Their conversation about a criminal matter pending against Edwards was overheard by a private party using a scanner that could be easily obtained by the general public. The intercepted conversation was tape recorded and the tape was given to the U.S. Attorney's Office in the Middle District of Louisiana. There, U.S. Attorney Bardwell listened to the tape and contacted the U.S. Attorney for the Eastern District of Louisiana, who refused to listen to the tape and notified Edwards' attorney about its existence. Edwards filed suit against U.S. Attorney Bardwell and the person who intercepted his conversation pursuant to 18 U.S.C.

185. *Id.* at 194–95.
186. *Id.* at 196.
187. *Id.* at 197–98.
188. *Id.* at 196–99.
189. *Id.*
190. *Id.* at 198. The district court had already made findings that two of the defendants were aware that conversations involving a mobile telephone could be overheard. Therefore, their conversations taking place over two mobile phones need not be suppressed. *Id.*
191. 632 F. Supp. 584 (M.D. La. 1986).

§ 2520, which creates a civil cause of action against anyone who wrongly intercepts or discloses a wire or oral communication.[192]

The district court disagreed with the reasoning of *Hall*, stating that:

> With all deference to the Ninth Circuit, this court considers that when either end of a communication originates over a radio telephone, that conversation is an "oral" communication and the fact that the communication travels in part on a line to a land-line telephone and back to a radio transmitter does not convert it to a "wire" communication. There is no reasonable expectation of privacy in a communication which is broadcast by radio in all directions to be overheard by countless people who have purchased and daily use receiving devices such as a "bearcat" scanner or who happen to have another mobile radio telephone tuned to the same frequency.[193]

The court held that neither the interception of the conversation nor the disclosure to the U.S. Attorney violated the Federal Wiretap Act. Accordingly, Edwards' suit was dismissed on summary judgment.[194]

While *Hall* and *Edwards* considered the application of the Federal Wiretap Act to interception of mobile telephone conversations, other courts faced similar issues involving portable telephone conversations. In *State v. Howard*,[195] a neighbor's AM/FM radio picked up the defendant's cordless telephone conversations.[196] The neighbor recognized the speaker's voice and recorded some of the conversations, which involved illegal drugs. The neighbor told the police, and agreed to record any additional conversations that he heard over his radio. The defendant was eventually arrested and charged with several drug offenses. At trial, the judge suppressed evidence of the telephone conversations and also suppressed evidence obtained from a search of the defendant's home. The State filed an interlocutory appeal.[197]

The Supreme Court of Kansas ruled that:

> [T]he term "wire communication," as defined in 18 U.S.C.A. § 2510(1), should be construed to apply only to that portion of a radio-telephone communication which is actually transmitted by the wire and not broadcast in a manner available to the public. We hold that those portions of the cordless telephone conversations

192. *See* 18 U.S.C. § 2520 (2000).
193. 632 F.Supp. at 589.
194. *Id.*
195. 679 P.2d 197 (Kan. 1984).
196. *Id.* at 198.
197. *Id.*

> intercepted by an ordinary FM radio in this case did not fall into the category of a "wire communication," but were in fact oral communications and that the rules pertaining to the interception of oral communications prescribed in Title III are applicable.[198]

The court further held that the defendant did not have a reasonable expectation of privacy in the broadcast portion of the conversation because the cordless telephone owner's manual fully explained the nature of the telephone.[199] Based on this analysis, the court concluded that evidence of the telephone conversations was admissible at trial.[200]

The Supreme Court of Rhode Island reached the same conclusion under a similar fact pattern in *State v. Delaurier*.[201] The court rejected the reasoning of *Hall* and agreed with the conclusion in *Howard* to the effect that the broadcast portion of a portable telephone conversation is an oral communication as defined by the Federal Wiretap Act.[202]

But the court did not reach the question of whether the defendant had a reasonable expectation of privacy in his oral communication. Rather, the court focused on the Federal Wiretap Act's prohibition of the interception of wire and oral communications, relying on 18 U.S.C. § 2510(4)'s definition of "interception" as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[203] The court held that an ordinary radio, which picked up the portable telephone broadcasts, was not a "device" as defined by the statute.[204] Therefore, all other issues become moot and the evidence was admissible.

The decisions in *Hall*, *Edwards*, *Howard*, *and Delaurier* all struggled with the need to categorize a broadcast communication as either "wire" or "oral." If oral, then the court had to determine whether the parties had a reasonable expectation that the communication was not subject to interception (except for *Delaurier*, which avoided this issue). Because the drafters of the Federal Wiretap Act did not anticipate the rapid growth of wireless technologies, the courts were forced to apply a statute that was becoming increasingly out of date.

198. *Id.* at 206.
199. *Id.*
200. *Id.*
201. 488 A.2d 688 (R.I. 1985).
202. *Id.* at 693–94.
203. *Id.* at 695.
204. *Id.* at 693–95.

3. The Electronic Communications Privacy Act Amends the Federal Wiretap Act to Protect the Privacy of "Electronic Communications"

a. The Privacy of Cellular Telephone Conversations and Email Falls Within the Protection of the Statute as Amended

In 1986, the Electronic Communications Privacy Act (ECPA)[205] amended the Federal Wiretap Act to extend privacy protections to "electronic" communications such as email while redefining "wire" and "oral" communications. The statutory amendments established a privacy interest for parties to cellular telephone conversations, but created serious ambiguities as to the extent of protection afforded to email and other emerging forms of communication.

18 U.S.C. § 2511 as amended by the ECPA states:

> Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> . . .
>
> (b) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> . . .
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).[206]

18 U.S.C. § 2510 as amended by the ECPA states:

> As used in this chapter—
>
> (1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station)

205. Pub. L. No. 99-508, 100 Stat. 1848 (1986).
206. 18 U.S.C. § 2511 (Supp. IV 1986).

> furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
>
> (2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;
>
> . . .
>
> (12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
>
> (B) any wire or oral communication . . .[207]

The amended version of 18 U.S.C. § 2510(1) effectively included cellular telephone conversations within the definition of "wire communication" and so prohibited the interception of cellular telephone conversations without judicial authorization. The legislative history of the ECPA declares:

> [18 U.S.C. § 2510(1) as amended] specifies that the use of wire, cable or other similar connections for the transmission of communications includes the use of such connections in a switching station. This subparagraph makes clear that cellular communications—whether they are between two cellular telephones or a cellular telephone and a "land line" telephone are included in the definition of "wire communications" and are covered by the

207. 18 U.S.C § 2510 (Supp. IV 1986).

> statute. As noted below, the bill distinguishes between cordless and cellular telephones.[208]

While creating a statutory privacy interest in cell phone conversations, the 1986 amendments to 18 U.S.C. § 2510(1) expressly excluded the "radio portion of a cordless telephone communication transmitted between the cordless telephone handset and the base unit" from the definition of a wire communication. The Senate Report explained the rationale for this distinction, asserting that "[b]ecause communications made on some cordless telephones can be intercepted easily with readily available technologies, such as an AM radio, it would be inappropriate to make the interception of such a communication a criminal offense. The wire portion of a cordless communication remains fully covered, however."[209]

Likewise, the 1986 amendments to 18 U.S.C. § 2510(2) effectively removed the radio portion of a cordless telephone conversation from the definition of oral communication. Senate Report 99-541 explains that Congress disapproved of the analysis in cases such as *Howard*, which offered protection if the court found that the participants had a reasonable expectation of privacy in a cordless telephone conversation. The Senate Report goes on to assert:

> [18 U.S.C. § 2510(2) defining "oral communications" is amended] to exclude electronic communications. There have been cases involving radio communications in which the court, having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The bill rejects that analysis by excluding electronic communications from the definition of oral communications.
>
> An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, not by an electronic medium.[210]

Lastly, the 1986 amendments to 18 U.S.C. § 2510(12) expressly removed the radio portion of a cordless telephone conversation from the definition of electronic communication.[211] Thus, the radio portion of a

208. S. REP. NO. 99-541, *supra* note 179, at 11, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3565.
209. *Id.* at 12, *reprinted in* 1986 U.S.C.C.A.N. at 3566.
210. *Id.* at 13, *reprinted in* 1986 U.S.C.C.A.N. at 3567.
211. *Id.* at 14, *reprinted in* 1986 U.S.C.C.A.N. at 3568.

cordless telephone conversation was excluded from statutory protection as a wire, oral, or electronic communication.

b. Although the Privacy of Electronic Communication is Protected by Statute, it does not Receive the Same Level of Protection as is Afforded to Wire Communication

Although the Federal Wiretap Act provides similar protection for wire, oral, and electronic communications, there are additional protections afforded to wire and oral communications that are not applicable to electronic communications. 18 U.S.C. § 2516(1) permits only certain designated high-ranking Justice Department officials to request authorization to intercept wire or oral communications as part of the investigation of an extensive list of specifically enumerated offenses.[212] In contrast, 18 U.S.C. § 2516(3) permits a wider range of government attorneys to request authorization for the interception of electronic communications as part of the investigation of any federal felony.[213]

It is significant to note that the ECPA did not update the statutory exclusionary rule of 18 U.S.C. § 2515, which makes evidence of wire or oral communications intercepted in violation of the Federal Wiretap Act inadmissible in court.[214] Therefore, the statutory exclusionary rule does not extend to electronic communications.[215] In the absence of a statutory exclusionary rule, illegally intercepted electronic communications are subject only to the Fourth Amendment exclusionary rule.

As a result, electronic communications receive less protection than wire communications in that illegal interception by private parties would not result in suppression under Fourth Amendment analysis, which only limits the actions of government officers. Moreover, some electronic communications that are illegally intercepted by government officers may be admissible under Fourth Amendment analysis due to the good faith exception to the constitutional exclusionary rule.[216] But even in the absence of a statutory exclusionary rule applicable to electronic communication, evidence of illegally intercepted electronic communications may nevertheless be inadmissible in court. 18 U.S.C. § 2511(1)(c) provides

212. 18 U.S.C. 2516 (1) (2000).

213. 18 U.S.C. § 2516(3).

214. *Compare* 18 U.S.C. § 2515 (1982) *with* 18 U.S.C. § 2515 (Supp. IV 1986) (relevant language unchanged).

215. S. REP. NO. 99-541, *supra* note 179, at 23, *reprinted in* 1986 U.S.C.C.A.N. at 3577.

216. *See* United States v. Leon, 468 U.S. 897 (1984); Massachusetts v. Sheppard, 468 U.S. 981 (1984). Michael Leib makes a convincing argument for amending the statutory exclusionary rule to treat electronic communication in the same manner as wire and oral communications. Michael Leib, *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. ON LEGIS. 393 (1997).

criminal penalties for disclosure of the contents of an illegally intercepted electronic communication.[217] It follows that a court should not play a role in the commission of a crime by permitting witness testimony that violates a criminal statute.[218]

As will be discussed in Section V.C., *infra*, electronic communications that have reached their destination and are held in electronic storage no longer receive the protection of the Federal Wiretap Act. Rather, the statutory scheme as interpreted by the courts distinguishes between the illegal interception of electronic communications during transmission and unlawful access to an electronic communication held in storage by a provider of electronic communication services. These stored electronic communications are governed by the far lesser protections of the Stored Communications Act.

4. The Telephone Disclosure and Dispute Resolution Act, Followed by the Communications Assistance for Law Enforcement Act, Further Amend the Federal Wiretap Act to Provide Additional Protection for Cellular Telephone Conversations and to Protect Cordless Telephone Conversations

As the use of wireless technology became more widespread, Congress enacted additional legislation to further protect the privacy of people conducting conversations over cellular and cordless telephones. Section 403 of the Telephone Disclosure and Dispute Resolution Act of 1992,[219] codified at 47 U.S.C. § 302a, ordered the Federal Communications Commission to issue regulations prohibiting the manufacture or importation of radio scanners that have the ability to receive cellular telephone transmissions.

In 1994, section 202 of the Communications Assistance for Law Enforcement Act (CALEA)[220] amended 18 U.S.C. § 2510 by deleting the language that excluded the radio portion of cordless telephone communications from the protection of the statute. Although the statute does not expressly state that the radio portion of cordless telephone conversations falls within its protections, House Report 103-827 explains that "[t]he protections of the Electronic Communications Privacy Act of 1986 are

217. 18 U.S.C. § 2511(1)(c) (2000).

218. David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail*, 11 GEO. J. LEGAL ETHICS 459, 477 (1998). *See also Nardone*, 302 U.S at 276 (discussing section 605's prohibition against divulging the contents of a wiretapped conversation "[t]o recite the contents of the message in testimony before a court is to divulge the message").

219. Pub. L. No. 102-556, § 403, 106 Stat. 4181, 4195 (1992) (codified at 47 U.S.C. § 302a (Supp. V 1993)).

220. Pub. L. No. 103-414, § 202, 108 Stat. at 4290 (codified at 18 U.S.C. § 2510 (1994)).

extended to cordless phones."[221] This intention is repeated later in the report as well.[222]

However, the 1994 amendments do not make clear whether the radio portion of a cordless telephone communication should be treated as an oral, wire, or electronic communication. An interesting law review note points out that ambiguity in the Federal Wiretap Act leaves this question open.[223] Moreover, the Federal Wiretap Act leaves open the possibility that older cordless telephones based on early technology that unintentional interception may remain unprotected.[224] Logically, one would expect the radio portion of a cordless telephone conversation to be treated like a cellular telephone conversation and characterized as a wire communication. But the statutory scheme is not known for its logic.

Despite its flaws, the history of the Federal Wiretap Act regarding cellular and cordless telephones provides an interesting demonstration of the manner in which technology and law combine to establish a right of privacy. *Hall*, *Edwards*, *Howard*, and *Delaurier* illustrate the view that communications over a media deemed to be subject to easy and accidental interception are not worthy of a legally recognized privacy interest.

Nevertheless, the ECPA amended the Federal Wiretap Act to create a right of privacy in cellular telephone conversations. Subsequently, the Telephone Disclosure and Dispute Resolution Act of 1992 ordered a ban on the manufacture and importation of devices that are capable of intercepting cellular telephone communications. Similarly, the Communications Assistance for Law Enforcement Act amended the Federal Wiretap Act to create a privacy right in the broadcast portion of cordless telephone communications. Thus, it can be argued that the privacy of telephone conversations does not really originate from the technological security of the media of communication. Rather, privacy emanates from the statutes and judicial decisions that prohibit the interception of communications without judicial authorization and mandate criminal and civil penalties for anyone who intentionally intrudes on that privacy interest.[225]

Such an assertion may seem counter-intuitive. Most people probably assume that their conversations over a wire telephone are secure and will not be intercepted, though they feel somewhat less certain about portable

221. H. REP. NO. 103-827 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3490.

222. *Id.*, *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497–98.

223. Basil W. Mangano, Note, *The Communications Assistance for Law Enforcement Act and Protection of Cordless Telephone Conversations: The Use of Technology as a Guide to Privacy*, 44 CLEV. ST. L. REV. 99 (1996).

224. *Id.* at 116–17.

225. *See* Albert Gidari, *Privilege and Confidentiality in Cyberspace*, 13 COMPUTER LAW. 1 (Feb. 1996).

telephone conversations due to the nature of the technologies. Yet none of our common methods of communication are truly secure in the sense that third parties are physically unable to intercept our conversations. For example, it is relatively easy to obtain telephone wiretapping equipment.[226]

Of course, one could argue that the parties to a sensitive communication should employ technology that will prevent others from learning the contents of their messages. For example, sensitive communications can be encrypted, or scrambled, so that an unauthorized third party who intercepts a message cannot make sense of it. Such practices would be a prudent security precaution in many business situations. But exclusive reliance on technology without a legal assurance of privacy leads to an "arms race" in which the measure of security is no more than the ability of encryption software to defeat decryption software.[227] On the other hand, a privacy right that is founded in law will offer protection regardless of leadership in the "arms race" at any given time even though some people will inevitably violate the law at the risk of civil and criminal penalties.

This is not to say that it would be good policy to create a statutory right of privacy in media of communication that are so insecure that communications are often intercepted by accident.[228] But once a privacy right is created by statute or judicial decision, the protections should be the same regardless of the medium of communication. Thus, letters in the mail, telephone conversations, and email should all receive the same level of protection from surreptitious interception by law enforcement officers or private parties.

As has been shown, letters in the mail receive less protection under Federal Rule of Criminal Procedure 41[229] and 18 U.S.C.A. § 3103a[230] than telephone calls are afforded under the Federal Wiretap Act. Likewise, the Federal Wiretap Act provides email with less protection from governmental intrusion than is provided to telephone calls. These distinctions cannot be justified. When the police surreptitiously learn the

226. For example, as of January 2004 a search on any internet search engine returns thousands of pages selling wiretap equipment.

227. The use of encryption software does not create a reasonable expectation of privacy for purposes of the Fourth Amendment. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN L. REV. 503 (2001).

228. Cordless phones are evolving to lessen the likelihood that the broadcast portion of a conversation will be accidentally intercepted. For example, cordless phones now broadcast on frequencies that will not be picked up on conventional radios. United States v. Smith, 978 F.2d 171, 177–79 (5th Cir. 1992).

229. FED. R. CRIM. PRO. 41 (2003).

230. 18 U.S.C.A. § 3103a (Supp. 2003).

contents of a communication, they intrude upon the same privacy interest regardless of the medium of communication. Therefore, the same protections should apply.

C. *Inconsistent Statutory Provisions Lead to Confusion about Interception of Email during Transmission and Access to Email in Storage; Additional Confusion about Access to Voicemail*

Part V.B.3., *supra*, explained that the ECPA extended some, but not all, Federal Wiretap Act protections to electronic communications. Moreover, the ECPA added Chapter 121 to Title 18 of the U.S. Code.[231] Chapter 121 is commonly known as the Stored Communications Act. It governs voicemail and email that is held in electronic storage for the recipient. Thus, the statutes draw a distinction between intercepting a wire or electronic communication while it is in transmission and intruding upon that same communication once it has reached its destination and is held in electronic storage.

18 U.S.C. § 2701 as added by the ECPA states:

> (a) Offense. Except as provided in subsection (c) of this section whoever—
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided by subsection (b) of this section.[232]

The Stored Communications Act generally prohibits Internet Service Providers from disclosing the contents of incoming or outgoing email. 18 U.S.C. § 2702 states:

> (a) Prohibitions. Except as provided in subsection (b)—

231. Pub. L. No. 99-508, 100 Stat. 1848, 1860–68 (codified at 18 U.S.C. §§ 2701–2710 (Supp. IV 1986)).

232. 18 U.S.C. § 2701 (Supp. IV 1986). The definition of "electronic storage" comes from the Federal Wiretap Act. 18 U.S.C. § 2510(17) (Supp. IV 1986) defined electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from . . ., a subscriber or customer of such service; and
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.[233]

The Stored Communications Act requires the Government to obtain a search warrant in order to compel an Internet Service Provider to disclose the contents of an email message held in electronic storage for 180 days or less. The Stored Communications Act provides less protection for email held in electronic storage for more than 180 days. As an alternative to a search warrant, the Government can compel the Internet Service Provider to disclose the contents of email through an administrative subpoena or court order. 18 U.S.C. § 2703, as it read in 1986 stated:

> (a) Contents of electronic communications in electronic storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications service for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
>
> (b) Contents of electronic communications in a remote computing service.

233. 18 U.S.C. § 2702 (2000).

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication. . . .
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
>
> (ii) obtains a court order for such disclosure under subsection (d) of this section;
>
> except that delayed notice may be given pursuant to section 2705 of this title.[234]

Criminal penalties for violation of the statute are set out in 18 U.S.C. § 2701(b)[235] and civil damages are authorized under 18 U.S.C. § 2707.[236] But 18 U.S.C. § 2708[237] expressly precludes any other remedies or sanctions for nonconstitutional violations of the statute. Significantly, the Stored Communications Act has no statutory exclusionary rule. Therefore, evidence obtained in violation of the Stored Communications Act is arguably admissible in court unless a constitutional exclusionary rule is implicated. The better view would prevent the introduction of any evidence obtained in violation of the Stored Communications Act, but the Act's exclusive remedies provision may weaken this position.[238]

The search warrant provisions of 18 U.S.C. § 2518 under the Federal Wiretap Act and 18 U.S.C. § 2703 under the Stored Communications Act lead to significant distinctions between the protection afforded to email while in transmission and the protection afforded to email that is in storage in the recipient's mailbox at his Internet Service Provider. For example, 18 U.S.C. § 2518(3) permits law enforcement officers to surreptitiously intercept email when they have received judicial authorization based on, *inter alia*, probable cause and a showing that

234. 18 U.S.C. § 2703 (Supp. IV 1986).
235. *Id.* § 2701(b).
236. *Id.* § 2707.
237. *Id.* § 2708.
238. Nevertheless, one can envision situations where the courts would refuse to permit the introduction of evidence obtained in violation of the statute even in the absence of a constitutional violation. For example, privileged information obtained in violation of the statute should not be admissible regardless of the exclusive remedies provision of the Stored Communications Act. *See* Gidari, *supra* note 225, at 2.

normal investigative procedures have been tried and have failed or that they reasonably appear to be unlikely to succeed if tried or that they are too dangerous to even try.[239]

But according to 18 U.S.C. § 2703(a), law enforcement officers can search email stored in a person's mailbox for 180 days or less at an ISP pursuant to a search warrant "issued using the procedures described in the Federal Rules of Criminal Procedure." Therefore, the search can be conducted surreptitiously through compliance with Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 3103a,[240] which does not require consideration of alternative investigative techniques before conducting a covert search.[241]

Rather, 18 U.S.C. § 3103a authorizes delayed notice of the execution of a search warrant if the court believes that contemporaneous notice would lead to an "adverse result," the warrant prohibits a seizure unless the court believes that the seizure is justified by reasonable necessity, and the warrant requires that notice be given within a reasonable time.[242] This "adverse result" standard does not require the court to make any finding about the possibility of employing less intrusive investigative techniques as an alternative to the covert search of stored email.[243] Such a finding would be required by 18 U.S.C. § 2518(3) if the police sought to intercept email during transmission. Moreover, other safeguards that are expressly spelled out by the Federal Wiretap Act governing interception of email during transmission are not included in the Stored Communications Act.[244]

There is no logical reason to provide greater protection against covert police surveillance for an email in transmission than for the same

239. 18 U.S.C. 2518(3) (2000).

240. *See supra* Part II.B. and text accompanying note 60. The Justice Department takes the position that it need not comply with 18 U.S.C. § 3103a in order to conduct the search without notice to the holder of the mailbox. The Justice Department theorizes that the statute merely requires notice to the Internet Service Provider. COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIM. DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, § III. D. 5 (July 2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (last visited June 16, 2003)[hereinafter SEARCHING AND SEIZING COMPUTERS]. This issue is discussed further in part V.C.1., *infra*.

241. If the email has been in the recipient's mailbox for more than 180 days, 18 U.S.C. §§ 2703 and 2705 allow law enforcement officers to conduct a surreptitious search pursuant to a subpoena or court order (rather than a search warrant) without consideration of alternative investigative techniques.

242. 18 U.S.C.A. § 3103a governs covert searches in general, adding more confusion to the issue. It is unclear whether intangibles such as email can be seized. *See* 4 LAFAVE, *supra* note 12, § 2.1(a), at 378.

243. *See supra* note 60.

244. *Compare* 18 U.S.C. § 2518 (2000) (setting out detailed procedures) *with* 18 U.S.C. § 2703 (2000) (exhibiting lesser safeguards).

email after it has reached the recipient's mailbox at his Internet Service Provider. In this regard, the statutory scheme lacks a coherent framework.[245]

It seems that the drafters of the statute were unable to anticipate a basic difference between telephone conversations and email messages. A telephone conversation can only be monitored while it is taking place since there is no permanent record left after the conversation ends. Similarly, an email message can be intercepted in transmission as it travels from sender to recipient. But the message can also be accessed while it is stored in the recipient's mailbox. In this respect, an email message shares some characteristics of a paper letter in that they both constitute a more permanent record than a phone call.

This article asserts that the same level of protection from covert surveillance should attach to communications by telephone, email, or conventional mail. Regardless of the medium of communication, surreptitious governmental intrusion upon the private exchange of ideas should be regulated by the same standard because the privacy interest is one and the same.

Berger[246] did not explain why the Supreme Court assumed that telephone conversations deserved greater protections against police wiretapping than are afforded to letters in the mail. Maybe the court assumed that the real-time nature of the interception of a telephone call was somehow more intrusive than covert interception of letters in the mail. But the intrusive nature of the wiretap does not come from the fact that it is contemporaneous with the communication. Rather, the highly intrusive aspect of the telephone wiretap derives from the fact that the police surreptitiously intercept private communications, implicating a First Amendment right that was recognized with respect to the mail in *Van Leeuwen*.[247]

If so, then the constitutional protections for wire communications set out in *Berger* as codified and expanded by the Federal Wiretap Act should be equally applicable to the mail and electronic communications as well. It follows that the same safeguards against covert police surveil-

245. To avoid the more stringent limitations on searches of email messages in transmission, law enforcement officers may simply seek judicial approval for access to the same messages in electronic storage once they reach the recipient's inbox. Gregory L. Brown, *Steve Jackson Games, Inc. v. United States Secret Service: Seizure of Stored Electronic Mail is not an "Interception" Under the Federal Wiretap Act*, 69 TUL. L. REV. 1381, 1390 (1995).

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

247. *See* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970).

lance should govern all media of communication that are deemed deserving of protection.[248]

As computer technology continues to converge with telecommunications technology, arbitrary statutory distinctions will lead to illogical results. For example, Michael Leib points out that if any part of a communication is deemed to be "wire" or "oral," then the entire communication is deemed to be "wire" or "oral," even if the communication is predominantly "electronic."[249] Therefore, internet telephony communications between a person using a computer and another person using a telephone should be treated as a wire communication. Unless wire and electronic communications are governed by the same rules, the courts will be forced to draw the same type of arbitrary distinctions as when they struggled to determine the privacy rights of people who used a mobile telephone or cordless telephone to speak to someone using a wire telephone.[250]

1. Judicial Treatment of Stored Email under Inconsistent Provisions in the Federal Wiretap Act and the Stored Communications Act

Arguably the leading decision in the area of police searches of email is *Steve Jackson Games, Inc. v. United States Secret Service*.[251] The case involved the search of email held on a server at a privately owned business. Steve Jackson Games, Inc. published books, magazines, and games. It established an electronic bulletin board on one of its computers, where it posted public information about its products. The bulletin board also permitted customers to send and receive private email.[252] Email addressed to a customer was "temporarily" stored on the hard drive of the computer running the bulletin board. The recipient could access his messages via computer and modem from other locations. The recipient then had the option to either delete the messages or to store them on the hard drive of the Steve Jackson Games computer.[253]

The Secret Service suspected a Steve Jackson Games employee of involvement in the unauthorized duplication and distribution of a file

248. Michael Leib argues that electronic communication receives a lower level of protection than oral and wire communication as the result of a political compromise that was necessary to obtain Justice Department approval of the Electronic Communications Privacy Act. Unless the Justice Department endorsed the proposed legislation, it was not likely to be signed into law during the Reagan Administration. *See* Leib, *supra* note 216, at 409–11. Even so, this does not explain the difference in treatment for email in transmission and email stored in the recipient's mailbox.

249. *Id.* at 415–17.

250. *See supra* Part V.B.2.

251. 36 F.3d 457 (5th Cir. 1994).

252. *Id.* at 458.

253. *Id.*

containing proprietary corporate information. Believing that a copy of the file might be found on the Steve Jackson Games bulletin board, the Secret Service obtained a search warrant authorizing the seizure of computer hardware and also authorizing its agents to read the information stored therein.[254]

Subsequently, several people who maintained email accounts through Steve Jackson Games filed suit against the Secret Service. These plaintiffs asked for damages as authorized by the Federal Wiretap Act and the Stored Communications Act.[255] The district court found that Secret Service agents read and deleted private email from the computer they had seized. The district court went on to award statutory damages under the Stored Communications Act, but held that the email was not "intercepted" as the word is used in the Federal Wiretap Act.[256] The plaintiffs appealed to the Fifth Circuit in order to recover greater statutory damages pursuant to the Federal Wiretap Act.[257]

The Fifth Circuit described the issue before it as "whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an 'intercept' proscribed by 18 U.S.C. § 2511(1)(a)."[258] In affirming the district court, the Fifth Circuit held that interception does not take place where a stored electronic transmission is seized before it is read by the intended recipient.[259] The Fifth Circuit reached this conclusion by focusing on a key distinction between the definitions of "wire communication" and "electronic communication" as set out in the Federal Wiretap Act.[260]

In essence, the court reasoned that the Federal Wiretap Act defined "intercept" so as to include the "aural *or other* acquisition of the contents of . . . wire, *electronic*, or oral communications."[261] The court went on to note that the definition of wire communication includes any electronic storage of a wire communication.[262] In contrast, the definition of electronic communication does not likewise include any electronic storage of an electronic communication.[263] Based on this distinction, the court con-

254. *Id.* at 458–59.
255. The plaintiffs also alleged violation of the Privacy Protection Act, which is not relevant to this discussion. *See Id.* at 459.
256. *Id.* at 459–60.
257. *Id.*
258. *Id.* at 460.
259. *Id.* at 460–63.
260. *Id.* at 461–62.
261. *Id.* at 461 (emphasis added).
262. *Id.*
263. *Id.*

cluded that Congress did not intend the law governing interception to be applicable to electronic communications that are in electronic storage.[264]

The court went on to buttress this conclusion by discussing the Stored Communications Act, which expressly governs unauthorized access to electronic communication in electronic storage. Since the Stored Communications Act was plainly applicable, the court reasoned that the Federal Wiretap Act was not controlling.[265]

Steve Jackson Games illustrates some of the problems inherent in the statutory scheme. The decision makes clear that the greater protection of the Federal Wiretap Act applies to the interception of email that is in transmission, while the lesser protection of the Stored Communications Act is applicable to email in electronic storage. The court articulated some of the differences in the statutory protections. For example, the court noted that the Federal Wiretap Act imposes strict time limits during which the eavesdropping can be conducted, and also requires law enforcement officers to minimize any monitoring of communications not relevant to the investigation.[266] Neither of these matters is addressed by the Stored Communications Act.

These arbitrary statutory distinctions overlook the basic privacy interest at issue. The intended recipient of an email message has the same privacy interest regardless of whether law enforcement officials intercept the message while it is in transmission or whether law enforcement officials access it after it has already arrived in the recipient's electronic mailbox. Since the privacy interest is the same, one would expect the protections of the privacy interest to be the same.

The rejection of this basic principle is reminiscent of the discredited rationale of *Olmstead*, which denied Fourth Amendment protection against wiretaps conducted without a physical trespass into a person's home or office.[267] In *Olmstead*, the Supreme Court was willing to offer protection against a trespass, but was unwilling to recognize a privacy interest in communications traveling over the public telephone lines.[268] Conversely, the current statutory scheme sets out greater safeguards against the interception of an electronic communication traveling over the public Internet than it sets out against electronic trespass to a person's electronic mailbox for the purpose of reading that same communication in storage.[269] And as will be discussed, the statutory protections against interception of an electronic communication during

264. *Id.* at 461–62.
265. *Id.* at 462–63.
266. *Id.* at 463.
267. 277 U.S. 438 (1928); *see* discussion *supra* Part IV.A.
268. *Olmstead*, 277 U.S. at 465–66.
269. *See supra* note 9.

transmission are likewise substantially greater than the protections against law enforcement agents covertly breaking into an office to read that same communication in storage on the hard drive of a personal computer.[270]

In a thoughtful and interesting effort to provide a logical explanation for these different statutory safeguards, Orin Kerr argues that the law often distinguishes between the treatment of prospective and retrospective searches.[271] Prospective searches, such as wiretaps, seek evidence that did not yet exist at the time the warrant was issued. Therefore, prospective searches raise more serious privacy concerns than the traditional retrospective search for evidence that already exists when the warrant is sought. Kerr asserts that a prospective search of a computer network is particularly intrusive because the police cannot know in advance just what email they will discover coming into or out of the suspect's electronic mailbox.[272] Of course, much of it may be irrelevant to the investigation. However, Professor Kerr claims that a retrospective search for stored email is usually less intrusive because many relevant messages may have been deleted.[273]

Professor Kerr makes an interesting argument, but the better view is that a person has the same privacy interest in his email whether it is intercepted during transmission or accessed from storage in his electronic mailbox. And regardless of whether the search is conducted prospectively or retrospectively, the police are likely to obtain email that is irrelevant to the investigation. For example, the retrospective search conducted in *Steve Jackson Games* clearly obtained a great deal of material that was irrelevant to the investigation. Moreover, the possibility that a retrospective search for stored email may be unsuccessful because some messages have been deleted does not lessen the impact of the intrusion into the privacy of the person under investigation.

Professor Kerr looks to the prospective or retrospective nature of the search in order to justify the difference in statutory protection. But it would be better to look at whether the search is conducted surreptitiously without contemporaneous notice to the person being subjected to the search. If so, law enforcement officers should be held to a higher standard than would govern their actions when they give contemporaneous notice of the search.

Of course, prospective searches of emails in transmission must be conducted in secret without contemporaneous notice because no suspect

270. *See infra* Part VII.

271. Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: the Big Brother that Isn't*, 97 NW. U. L. REV. 607, 616–18 (2003).

272. *Id.*

273. *Id.*

would send incriminating emails if he knew that they would be intercepted by the police. But retrospective searches for stored email can be conducted with or without contemporaneous notice. This article asserts that retrospective law enforcement access to stored email without notice to the holder of the mailbox constitutes the same invasion of privacy as prospective law enforcement interception of a message during transmission. If so, then both should be afforded the same protections of the *Berger* standards as codified in the Federal Wiretap Act. On the other hand, lesser safeguards are sufficient if law enforcement officers give contemporaneous notice to the mailbox holder when they conduct a retrospective search for stored email.

The highly technical language of the Federal Wiretap Act and the Stored Communications Act lead to additional distinctions in the treatment of email without regard to the underlying privacy interests. It is important to note that *Steve Jackson Games* addressed the statutory treatment of email stored in the recipient's electronic mailbox before the recipient actually read it. The more recent decision in *Fraser v. Nationwide Mutual Insurance Co.*[274] had the opportunity to further confuse matters when it was faced with issues of statutory construction as applied to email that had already been read by the recipient.

Fraser was an insurance agent with Nationwide, which provided an email system for use by its agents. Company officials suspected Fraser of contract violations. An information technology employee searched through stored email in the accounts of Fraser and other agents to discover evidence of Fraser's activities. Fraser sent a particular message to an agent named McAllister that revealed a potential contract violation. A stored copy of the message was retrieved from McAllister's electronic mailbox on Nationwide's server even though McAllister previously retrieved and deleted his copy of it.[275]

Nationwide fired Fraser. His subsequent lawsuit against Nationwide alleged violations of the Federal Wiretap Act and the Stored Communications Act. The court reasoned that the Federal Wiretap Act generally prohibits interception of email during the course of transmission. After an extended discussion of the way email works, the court concluded that a message remains in transmission after it has reached the recipient's mailbox but has not yet been retrieved. Once the message has been retrieved, it is no longer subject to the provisions of the Federal Wiretap Act. Since McAllister had already retrieved the message, the copy that

274. 135 F. Supp. 2d 623 (E.D. Pa. 2001).
275. *Id.* at 627–31.

nevertheless remained on the server was not governed by the Federal Wiretap Act.[276]

The court also reasoned that the Stored Communications Act generally prohibits unauthorized access to email in electronic storage.[277] But the statutory definition of electronic storage is limited to temporary, intermediate storage incidental to transmission as well as storage for purposes of backup protection. Based on its discussion of how email works, the court believed that the message found on the server was not in intermediate storage.[278] Nor did it qualify as a backup, which the court viewed as a copy that an email system stores only while a message is in transmission as protection in case the system crashes before transmission is completed. Therefore, it was not subject to the protection of the Stored Communications Act.[279]

By focusing on the technology rather than on the underlying policy, the court reached a poor result. Further application of the court's analysis would unavoidably lead to some unintended consequences. For example, consider that 18 U.S.C. § 2511(1)[280] generally prohibits the interception of electronic communication such as email. And 18 U.S.C. § 2701(a)[281] generally prohibits unauthorized access to electronic communication held in electronic storage. Under the logic of *Fraser*, a "hacker" who electronically breaks into an Internet Service Provider's network and reads email that has already been viewed by the intended recipient has violated neither statute.

Similarly, consider that 18 U.S.C. § 2518[282] sets out the procedure for law enforcement officers to request authorization to intercept electronic communications. Also consider that 18 U.S.C. § 2703[283] sets out the procedure for law enforcement officers to request authorization to gain access to stored electronic communications. Under the logic of *Fraser*, neither statute gives law enforcement officers the power to request judicial authorization to read email that has already been viewed by the recipient. Yet if law enforcement officers hacked into the network and obtained the message without prior judicial approval, neither statute would have been violated.

The Justice Department takes a somewhat more nuanced approach. The Computer Crime and Intellectual Property Section of the Criminal

276. *Id.* at 631–35.
277. *Id.* at 635–36.
278. *Id.* at 637.
279. *Id.*
280. 18 U.S.C. § 2511(1) (2000).
281. *Id.* § 2701(a).
282. *Id.* § 2518.
283. *Id.* § 2703.

Division provides comprehensive advice to U.S. Attorneys on interpreting the Federal Wiretap Act and the Stored Communications Act.[284] The Justice Department focuses on the statutory definition of "electronic storage" as limited in scope to "temporary, intermediate storage of a[n] . . . electronic communication incidental to electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection."[285] The Justice Department also focuses on the statutory distinction between an "electronic communication service" and a "remote computing service."[286]

For all practical purposes, an Internet Service Provider, which offers Internet access and email accounts to its subscribers, qualifies as a provider of electronic communication service. An example of a provider of remote computing service is the iDisk service offered by Apple Computer, which allows subscribers to store files online so they can be accessed by the subscriber from multiple locations.[287] A person might use a remote computing service to facilitate access to his files while traveling or to store files for backup protection.

The Justice Department uses an illustration to make sense of a very complicated analysis.[288] A similar illustration will demonstrate the Justice Department's analysis for purposes of this article. This illustration will consider email held in an account with America Online, an ISP available to the general public. This will be compared to email held in an account at the University of Idaho, which provides Internet access only to faculty, staff, and students, but not to the general public.

If a person leaves unopened email in his mailbox at America Online or at the University of Idaho for 180 days or less, then 18 U.S.C. § 2703(a) requires law enforcement officers to obtain a search warrant in accordance with the federal rules of criminal procedure in order to gain access to those messages.[289] The Justice Department argues that according to 18 U.S.C. § 2703(b)(1)(A), law enforcement officers who obtain a search warrant based on probable cause pursuant to Fed. R. Crim. Pro. 41 need not provide contemporaneous notice to the mailbox holder.[290]

In contrast, the Justice Department argument leads to the result that unopened email in a person's mailbox at America Online or at the University of Idaho for more than 180 days is subject to lesser

284. *See* SEARCHING AND SEIZING COMPUTERS, *supra* note 240.
285. *Id.*; *see* 18 U.S.C. § 2510(17) (2000).
286. *Compare* 18 U.S.C. § 2510(15) (2000) *with* 18 U.S.C. § 2711(2) (2000).
287. *See* http://www.mac.com. (advertising "[t]ransfer files too large to email, exchange documents. . . or just store files online.") (last visited October 17, 2003)
288. *See* SEARCHING AND SEIZING COMPUTERS, *supra* note 240, § III B.
289. *Id.* at §§ III D, III F.
290. *Id.*

protections under 18 U.S.C. § 2703(b)(1)(B), permitting law enforcement access pursuant to search warrant without notice to the mailbox holder, or upon issuance of a subpoena or court order as alternatives to a search warrant.[291]

Of course, access pursuant to subpoena or court order would normally require contemporaneous notice to the owner of the email account. However, the statute also provides for access without contemporaneous

291. *Id.* at § III F. The Justice Department is mistaken in asserting that law enforcement officers need only serve a search warrant on the ISP in compliance with FED. R. CRIM. PRO. 41 and need not provide notice to the mailbox holder. 18 U.S.C. § 2703(a), governing access to unopened email stored for 180 days or less, requires law enforcement officers to obtain "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." There is no mention of access without notice to the mailbox holder. A more reasonable interpretation of the statute would require law enforcement officers to give contemporaneous notice to the mailbox holder. 18 U.S.C. § 2703(a) goes on to mandate that law enforcement officers can obtain access to unopened email stored for more than 180 days by any means authorized under 18 U.S.C. § 2703(b). 18 U.S.C. § 2703(b)(1)(A) authorizes law enforcement officers to gain access to unopened email stored for more than 180 days "without required notice to the subscriber or customer" if they obtain "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."

Significantly, 18 U.S.C. § 2703(b) implies that contemporaneous notice to the mailbox holder is normally "required." Since 18 U.S.C. § 2703(a) makes no provision to delay the required notice to the mailbox holder when obtaining access to email stored for 180 days or less, it is logical to believe that contemporaneous notice is required.

It is important to consider that 18 U.S.C. § 2703(b) requires law enforcement officers to obtain a warrant in accordance with the totality of the Federal Rules of Criminal Procedure in order to gain access to email stored more than 180 days without required notice to the mailbox holder. The Justice Department interprets this provision as merely requiring compliance with FED. R. CRIM. PRO. 41, concerning search and seizure in general. But a better interpretation would also require compliance with the additional procedural safeguards of 18 U.S.C. § 3103a concerning searches with delayed notice. This interpretation would be more in keeping with Dempsey's observation that as technology progresses, many of our most important records will not be "papers" stored in our houses, but will be electronic files accessed from remote locations. *See* Dempsey, *supra* note 9.

But even if law enforcement officers must comply with 18 U.S.C. § 3103a in conducting a search of email stored for more that 180 days without contemporaneous notice to the mailbox holder, the statutory safeguards are not as rigorous as those of 18 U.S.C. § 2518 concerning interception of communications during transmission. Thus, law enforcement officers can obtain a warrant for a surreptitious search of stored email without showing that alternative investigative techniques have been tried or would be unlikely to succeed or would be too dangerous. And there is no express requirement that law enforcement officers executing the search minimize their access to email not relevant to the investigation. Both of these safeguards would be applicable to law enforcement efforts to intercept email messages during transmission.

Once again, all of these technical distinctions resulting from efforts to interpret the statutory scheme serve no purpose if one accepts the assumption that the underlying privacy interest remains the same regardless of whether the message is intercepted during transmission, regardless of whether the message has been opened by the recipient, and regardless of whether the message has been stored for more than 180 days.

notice.[292] Thus, law enforcement officers can obtain surreptitious access even in the absence of a search warrant based on probable cause.

This disparity in protection against law enforcement searches makes little sense. If translated to physical searches of paper documents, an unopened letter stored in a file cabinet for 180 days or less in a person's office would be afforded greater protection from search and seizure than another unopened letter in the same drawer that was stored for more than 180 days.

The Justice Department's argument also leads to the result that if a person opens his email but leaves it in his mailbox at America Online, law enforcement officers can again obtain access through a subpoena or court order pursuant to 18 U.S.C. § 2703(b) as an alternative to a search warrant. The Justice Department reasons that the mailbox holder is using America Online not as his Internet Service Provider with respect to that opened email, but as a remote computing service in order to store his opened email. Since America Online is acting as a remote computing service and the opened email is no longer in "temporary, intermediate storage," it is no longer entitled to the search warrant requirement of 18 U.S.C. § 2703(a).[293]

But if a person opens his email and leaves it in his mailbox at the University of Idaho, the Justice Department would conclude that the Stored Communications Act no longer applies. Again, the Justice Department reasons that the mailbox holder is using the University of Idaho not as his Internet Service Provider with respect to that opened email, but as a remote computing service. However, the applicable statutory provisions only provide protection for files stored at a remote computing service that is available to the general public. Because the University of Idaho does not issue Internet accounts to the general public, law enforcement access to opened email is not regulated by statute.[294]

If the Justice Department interpretation is correct, then it follows that the Stored Communications Act does not prohibit a "hacker" or a law enforcement officer from accessing opened email in storage on a server by an Internet Service Provider that does not accept subscriptions from the general public. From here it could be argued that law enforcement officers do not need judicial authorization to access opened email in electronic storage at an ISP not available to the general public because the statute does not create any privacy interest. But the Justice Department does not take such an extreme position. Rather, the Justice Department argues that a subpoena is required before law enforcement

292. 18 U.S.C. §§ 2703(b)(1)(B), 2705 (2000).
293. SEARCHING AND SEIZING COMPUTERS, *supra* note 240, §§ III B, III F.
294. *Id.*

officers can obtain access to opened email at an ISP that is not available to the general public.[295]

While *Steve Jackson Games*, *Fraser*, and the Computer Crime Section's *Searching and Seizing Computers* concentrate on statutory interpretation, the military case of *United States v. Maxwell*[296] focuses on constitutional issues raised by the search of a person's email account. *Maxwell* may be the first case to recognize a reasonable expectation of privacy in a person's email account.

Air Force Colonel James Maxwell subscribed to America Online ("AOL") for email and other online services. AOL allowed its subscribers the opportunity to open up to five separate email accounts per subscription. Each account had its own unique user i.d., referred to as a "screen name" in AOL terminology, and its own password. Each email account made use of its own "mailbox."[297]

In 1991, a subscriber named Roger Dietz complained that child pornography was being distributed on AOL. Dietz claimed that he received email messages with pornographic images attached to them. AOL representatives contacted the FBI.[298]

Dietz was not the original recipient of the messages that he found objectionable. The headers indicated that the messages had been sent to others and forwarded on before they reached Dietz. By reading the headers, the messages could be traced from the originator through the recipients prior to Dietz. But the headers only revealed their screen names rather than their true identities.[299]

The FBI obtained a search warrant directing AOL to provide copies of all the email in the mailboxes corresponding to about 80 screen names taken from the headers of the messages. AOL was also ordered to identify the holders of the screen names.[300]

Because representatives of AOL and the FBI held preliminary discussions before the warrant was issued, AOL had a general idea of the information that would be demanded by the warrant before it was actually issued. Accordingly, AOL wrote a program to extract the necessary information from its computers. There was some question as to whether AOL ran the program before the warrant was served. Regardless, AOL's program provided the FBI with more information than was called for by the search warrant. Not only did AOL identify the subscribers and turn over all of the email in the mailboxes of the eighty listed screen names,

295. *Id.*
296. United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).
297. *Id.* at 411–12.
298. *Id.* at 412.
299. *Id.* at 412–13.
300. *Id.*

AOL also turned over email from all additional mailboxes belonging to those subscribers under their other screen names.[301]

Using the information from AOL, the FBI discovered that the screen name "Redde1," which was listed in the search warrant, belonged to Colonel Maxwell. The FBI also discovered that Colonel Maxwell had another mailbox under the screen name of "Zirloc." In the Zirloc mailbox, the FBI found messages that were sent to another Air Force officer discussing Colonel Maxwell's sexual preferences.[302]

The FBI contacted the Air Force Office of Special Investigations, which started its own investigation of Colonel Maxwell. Based on the original search warrant and the Zirloc email, the AFOSI obtained authorization from a military magistrate to search Colonel Maxwell's home for evidence related to "possession and transmission of child pornography and other obscene matter."[303] AFOSI agents seized Colonel Maxwell's computer and located three images involving child pornography.

At general court-martial, Colonel Maxwell was convicted of offenses connected with the images found on his computer and two additional offenses related to the Zirloc email.[304] The trial court decision was affirmed by the U.S. Air Force Court of Criminal Appeals.[305] But the U.S. Court of Appeals for the Armed Forces reversed the part of the conviction related to the Zirlock mailbox, holding that a person has a reasonable expectation of privacy in his email account.[306]

The court explained that a party to a telephone conversation has a reasonable expectation that the police will not monitor his conversation in the absence of prior judicial authorization.[307] And a person who mails a letter has a reasonable expectation that the police will not read it unless they first obtain a search warrant.[308] Nevertheless, a party to a telephone conversation runs the risk that the other party will reveal the substance of the conversation to the police or to others.[309] And a person who mails a letter runs the risk that the recipient will show it to someone else.[310]

Having made this analogy, the court went on to the logical conclusion:

---

301. *Id.* at 413.
302. *Id.* at 413–14.
303. *Id.* at 414.
304. United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996).
305. United States v. Maxwell, 42 M.J. 568 (A.F. Ct. Crim. App. 1995) (NO. ACM 30704).
306. United States v. Maxwell, 45 M.J. 406, 410–14, 423–24 (C.A.A.F. 1996).
307. *Id.* at 417.
308. *Id.*
309. *Id.* at 417–19.
310. *Id.* at 418.

> Drawing from these parallels, we can say that the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny. In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way.[311]

Therefore, Colonel Maxwell did not have a privacy interest in the messages that Dietz turned over to the FBI and so was not entitled to Fourth Amendment protection.[312] However, Colonel Maxwell had a reasonable expectation of privacy in the contents of each of his separate email accounts as stored on AOL's computers.[313] The search warrant authorized a search of the mailboxes corresponding to the 80 particular screen names taken from the FBI affidavit, but did not authorize a search of any other mailboxes used by the AOL subscribers under investigation. In the absence of authorization to seize email from the Zirloc mailbox, the Zirloc messages must be suppressed.[314]

Maxwell also raises other issues that the court did not discuss. The search warrant directed AOL to turn over to the FBI all email in the 80 listed mailboxes.[315] However, the Court of Appeals for the Armed Forces analogized email to a telephone conversation in finding a reasonable expectation of privacy. Significantly, *Berger* held, *inter alia*, that Fourth Amendment principles demand that judicial authorization to conduct a telephone wiretap must describe with particularity the conversations to be intercepted.[316] Based on this description, law enforcement officers must minimize their eavesdropping on irrelevant conversations.[317]

Likewise, the *Maxwell* search warrant should have imposed similar restrictions on email that is either intercepted in transmission or taken from electronic storage in the recipient's mailbox. Yet the warrant placed

311. *Id.*
312. *Id.* at 417–19.
313. *Id.* at 420.
314. *Id.* at 419–22.
315. *Id.* at 433.
316. *Berger v. New York*, 388 U.S. 41, 55–56 (1967).
317. *See*, Michael Goldsmith and Kathryn Ogden Balmforth, *The Electronic Surveillance of Privileged Communications: A Conflict in Doctrines*, 64 S. CAL. L. REV. 903, 924–35 (1991) (discussing minimization in the context of telephone wiretaps).

no limits on the email in Colonel Maxwell's mailbox that the FBI could read. Rather, it subjected all email in Colonel Maxwell's "Redde1" mailbox to review by the FBI. At the least, the authorization should have specified with particularity that the FBI was to focus on email that contained pornographic images while minimizing its intrusion into other messages.[318]

The *Berger* safeguards of particularity and minimization are codified by the Federal Wiretap Act at 18 U.S.C. § 2518(4)(c) and § 2518(5).[319] The Federal Wiretap Act applies these safeguards to the interception of telephone calls and also to the interception of electronic communication such as email. But the Stored Communications Act contains no corresponding protection governing law enforcement access to stored email.

This statutory distinction is unjustified. *Steve Jackson Games* tried to rationalize it by asserting that law enforcement officers are less likely to examine the entirety of all stored email messages in a person's mailbox because they can use technology to key word search through it and only read the relevant messages.[320] But the court believed that it is not possible to key word search through email as it is intercepted during transmission.[321] This position is not entirely accurate.

Intercepted email is normally stored on disk by law enforcement officers[322] and could be key word searched before they read any of it. In any event, law enforcement officers are not obligated to consistently implement any key word or other minimization strategy for stored email unless required to do so by statute or case law.

Maxwell correctly recognized a Fourth Amendment privacy interest in a person's email account. Surprisingly, *Maxwell* focused on the constitutional issue with no discussion of *Berger*. Nor did *Maxwell* discuss the Federal Wiretap Act or the Stored Communications Act. Having analogized email to a telephone conversation, the court should have addressed the need to apply the *Berger* safeguards to the email stored in Colonel Maxwell's "Redde1" account as a matter of constitutional law.[323]

---

318. Despite the broad language of the warrant, there is some indication that AOL only produced email that had attached graphics files. 45 M.J. at 413. But if so, then the FBI would not have discovered the Zirloc email containing a discussion of sexual preferences with no "questionable graphics files." *Id.* at 414.

319. 18 U.S.C. §§ 2518(4)(c), 2518(5) (2000).

320. *Steve Jackson Games*, 36 F.3d 457, 463. (5th Cir. 1994).

321. *Id.*

322. *See infra* Part VI.

323. Despite these criticisms, *Maxwell's* recognition of Fourth Amendment principles is sound and represents the better view. In contrast, Professor Kerr argues that courts are generally reluctant to extend Fourth Amendment protections to new communications technologies that are already safeguarded by statute. *See supra* Kerr, *supra* note 273, at 629–30.

2. Judicial Treatment of Voicemail under Inconsistent Provisions in the Federal Wiretap Act and the Stored Communications Act

The Ninth Circuit was squarely faced with inconsistencies in the provisions of the Federal Wiretap Act and the Stored Communications Act in *United States v. Smith*.[324] There, a corporate officer named Smith telephoned an employee named Bravo. Smith left a voicemail message revealing that he was engaged in illegal insider trading of PDA Engineering Corp. stock. It turns out that Bravo did not select a very secure password to protect her email account. Another employee, Gore, guessed Bravo's password and secretly accessed her mailbox for unknown reasons. Gore forwarded Smith's message to her own mailbox. Gore then tape recorded Smith's message and gave the recording to an employee named Phillips. He telephoned the U.S. Attorney's office and played it for an Assistant U.S. Attorney, who began a criminal investigation. Subsequently, Smith was convicted in federal district court. The court suppressed evidence of the stored voicemail message, but permitted the Government to present the rest of its evidence. The Ninth Circuit affirmed the conviction.[325]

Smith argued on appeal that the Federal Wiretap Act provided the controlling law. He claimed that the voicemail message had been illegally intercepted. Accordingly, the message and all evidence derived therefrom must be suppressed pursuant to 18 U.S.C. § 2515. The Ninth Circuit summarized Smith's argument as follows:

> Smith insists that the Wiretap Act controls. The district court agreed. Section 2515 provides, in relevant part, that "[w]henever any *wire . . . communication* has been *intercepted*, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial." 18 U.S.C. § 2515 (emphasis added). Section 2510(1) defines "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection" and expressly includes within its scope "any *electronic storage* of such communication." 18 U.S.C. § 2510(1) (emphasis added) [footnote omitted]. Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire . . . communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

---

324. 155 F.3d 1051 (9th Cir. 1998).
325. *Id.* at 1053–54, 1070.

> In view of the rather broad definitions supplied in § 2510, Smith argues, the voicemail message Gore retrieved from Bravo's mailbox seems rather plainly to fit within the language of the exclusionary provision of § 2515. For starters, the message itself, which Smith left in the voicemail system via telephone, was a "wire communication;" it was an "aural transfer," made using a wire facility (the telephone line), and was subsequently "electronic[ally] stor[ed]" within the voicemail system. In addition, Gore's act of recording the message with a handheld audiotape-recording "device" constituted an "aural or other acquisition" [footnote omitted] –and, hence, an "interception"–of the message. It is clear, Smith insists, that [section] 2515 applies.[326]

Smith's argument accurately stated the law according to the Federal Wiretap Act as it existed at the time. However, the Government answered with an equally accurate statement of the law pursuant to the Stored Communications Act:

> Section 2701, which is part of the Stored Communications Act, provides for the criminal punishment of anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains . . . access to a wire . . . communication while it is in storage in such system." 18 U.S.C. § 2701. There is no doubt that the voicemail message at issue is a "wire communication." [footnote omitted] We have also already observed that the message was in "storage" within PDA's voicemail system. When Gore used Bravo's password to dial into the voicemail system, and then retrieved and recorded Smith's message, the government argues, she violated § 2701's prohibition on "access[ing]" stored wire communications. Consequently, the government argues, the voicemail message fits within § 2701.
>
> The fact that § 2701, as well as § 2515, appears to apply to the voicemail message is significant, the government argues, because, unlike the Wiretap Act, the Stored Communications Act does *not* provide an exclusion remedy. It allows for civil damages, *see* 18 U.S.C. § 2707, and criminal punishment, *see* 18 U.S.C. § 2701(b), but nothing more. Indeed, the Stored Communications Act expressly rules out exclusion as a remedy; § 2708, entitled "Exclusivity of Remedies," states specifically that § 2707's civil cause of action and § 2701(b)'s criminal penalties

326. *Id.* at 1055.

> "are the *only* judicial remedies and sanctions for violations of" the Stored Communications Act. 18 U.S.C. § 2708 (emphasis added). Therein lies the rub. If the voicemail message at issue is subject to the strictures of the Stored Communications Act, then suppression is not an available remedy. If, however, it is subject to the Wiretap Act, then suppression is quite explicitly available. In other words, with respect to this case, the Wiretap Act and the Stored Communications Act appear, on their faces, to be mutually exclusive statutes (with mutually exclusive remedial schemes). Unfortunately, at least at first glance, Congress seems to have defied the laws of semantics and managed to make the voicemail message here at issue simultaneously subject to both. [footnote omitted][327]

In an attempt to reconcile the discrepancy, the Ninth Circuit concluded that the Stored Communications Act is a lesser included offense within the Federal Wiretap Act.[328] The court reasoned that a person can obtain access to a communications facility without actually discovering the contents of the communications stored therein.[329] A person who simply obtains access to the facility has violated the Stored Communications Act. But when that person goes further and actually learns the contents of stored communications, he has violated the Federal Wiretap Act.

The court reached this conclusion by concentrating on the words "intercept" in the Federal Wiretap Act and "access" in the Stored Communications Act. The court explained:

> The word "intercept" entails *actually* acquiring the contents of a communication, whereas the word "access" merely involves *being in position* to acquire the contents of a communication. In other words, "access[]" is, for all intents and purposes, a lesser included offense (or tort, as the case may be) of "intercept[ion]." As applied to the facts of this case, Gore might have violated the Stored Communications Act's prohibition on "access[ing]" by simply making unauthorized use of Bravo's voicemail password and roaming about PDA's automated voicemail system, even had she never recorded or otherwise "intercepted" the contents of any given message. Once she retrieved and recorded Smith's message, however, she crossed the line between the Stored Communications Act and the Wiretap Act and violated the latter's prohibition on "intercept[ion]."[330]

327. *Id.* at 1055–56 (emphasis in original).
328. *Id.* at 1058.
329. *Id.* at 1059.
330. *Id.* at 1058 (emphasis in original).

The court ultimately concluded that Gore had intercepted Smith's voicemail message in violation of the Federal Wiretap Act.[331] The evidence of the voicemail message was properly suppressed by the district court, while evidence derived from the voicemail was sufficiently attenuated as to be properly admissible as evidence.[332] This derivative evidence was sufficient to support the conviction.

The Ninth Circuit's interpretation of the Stored Communications Act is in error. 18 U.S.C. § 2701 states:

> (a) Except as provided in subsection (c) of this section whoever—
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[333]

According to the Ninth Circuit, a person commits an offense under the Stored Communications Act by intentionally gaining unauthorized access to an electronic communications service so as to be in a position to *obtain access* or *alter access* or *prevent authorized access* to a stored communication without actually reading the communication.[334]

The court's reading of the statute makes much of its language unnecessary. A person who obtains access to a communication that was not addressed to him or who prevents the intended recipient from obtaining access has altered access to that communication. Accordingly, the prohibition against placing oneself in a position to alter access would be sufficient to state the elements of the offense. The two other prohibitions would be redundant.

A better interpretation of the Stored Communications Act would say that a person commits a violation when he intentionally gains unauthorized access to an electronic communications service and actually *obtains* or *alters* a stored communication, or *prevents authorized access* to it. Such an interpretation is more consistent with the rest of the statute.

The Ninth Circuit's interpretation leads to unintended consequences for the statutory treatment of email because the Stored Communications Act treats email the same as voicemail. Specifically, the court's analysis

331. *Id.* at 1058.
332. *Id.* at 1059–63.
333. 18 U.S.C. § 2701 (2000).
334. *See* 155 F.3d 1051, 1058 (9th Cir. 1998).

leads to the conclusion that whenever someone gains unauthorized access to an electronic communication service provider and reads someone else's stored email, he has violated the Federal Wiretap Act as though the email has been intercepted during transmission.

It follows that *Smith* places a higher burden on law enforcement officers than is contemplated by the statutory scheme. Under the Ninth Circuit's reasoning, it would make no sense for the FBI to seek a warrant pursuant to the Stored Communications Act at 18 U.S.C. § 2703 because the Stored Communications Act only governs efforts to *put oneself into position* to surreptitiously read an email message. Assuming that the police want to *read* that message, they would have to comply with the more stringent provisions of the Federal Wiretap Act at 18 U.S.C. § 2518 governing interception of email.

Put another way, the Ninth Circuit's interpretation leads to the conclusion that all eavesdropping on wire or electronic communication is governed by the Federal Wiretap Act. If so, then law enforcement officers must comply with the strict standards of 18 U.S.C. § 2518 in seeking authorization to read a suspect's email regardless of whether that email is intercepted while in transmission or whether it is accessed from electronic storage in the recipient's mailbox at an Internet Service Provider. Therefore, the lesser warrant standards of 18 U.S.C. § 2703 become completely irrelevant to the statutory scheme despite its plain language setting out the procedure for obtaining judicial approval to read a suspect's stored email.

3. Judicial Treatment of Web Sites under Inconsistent Provisions in the Federal Wiretap Act and the Stored Communications Act

The Ninth Circuit continued to struggle with the implications of *Smith* when it decided *Konop v. Hawaiian Airlines*.[335] There, airline pilot Robert Konop created a web site critical of his employer and his union. Site visitors were required to log in with a user name and password. Konop assigned user names to certain employees, but not to representatives of management or his union. In order to obtain a password and view the web site, employees had to register and agree not to disclose the site's contents. Hawaiian Airlines Vice President James Davis viewed the web site by logging in with the names of two employees, who gave him permission to use their identities. Konop sued in federal district court. He alleged that when Davis viewed his secure web site under false pretenses, Davis intercepted an electronic communication in violation of the

335. 236 F.3d 1035 (9th Cir. 2001) [hereinafter *Konop I*], *opinion withdrawn by* 262 F.3d 972 (2001), *superseded by* 302 F.3d 868 (9th Cir. 2002) [hereinafter *Konop II*], *cert. denied* 537 U.S. 1193 (2003).

Federal Wiretap Act and unlawfully accessed stored communications in an electronic communications facility in violation of the Stored Communications Act. The district court granted summary judgment against Konop on these claims.[336]

On appeal, the Ninth Circuit initially held that Konop raised triable issues of fact as to whether Hawaiian Airlines violated the Federal Wiretap Act and the Stored Communications Act.[337] However, the opinion was subsequently withdrawn. In a new opinion, the Ninth Circuit held that Hawaiian Airlines did not violate the Federal Wiretap Act and affirmed the summary judgment against Konop with respect to that claim. Consistent with its earlier opinion, the Ninth Circuit again held that Konop could proceed with his claim under the Stored Communications Act.[338] The Ninth Circuit's change of heart illustrates the difficulties caused by the poorly drafted statutes. The original decision, *Konop I*, as well as the revised decision, *Konop II* will be discussed in detail.

In *Konop I*, the Ninth Circuit realized that the civil damages recoverable under the Federal Wiretap Act were substantially greater than the damages that might be awarded under the Stored Communications Act.[339] Accordingly, the court defined the issue before it as whether viewing a web site through false pretenses constitutes a violation of either or both statutes.[340]

The court considered the web site to be an electronic communication held in storage, and focused on the question of whether an electronic communication (here, a web page) could be intercepted for purposes of the Federal Wiretap Act while it was held in electronic storage on a web server. The Ninth Circuit disagreed with the Fifth Circuit's decision in *Steve Jackson Games*, which held that an interception must take place contemporaneously with the transmission of an electronic communication.[341]

The Ninth Circuit explained:

> An electronic communication in storage is no more or less private than an electronic communication in transmission. Distinguishing between the two for purposes of protection from interception is "irrational" and "an insupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA." [citation omitted]

336. *Konop I*, 236 F.3d at 1040–42.
337. *Id.* at 1040.
338. *Konop II*, 302 F.3d at 872.
339. *Konop I*, 236 F.3d at 1042.
340. *Id.*
341. *Id.* at 1044–46.

> . . .
>
> We believe that Congress intended the ECPA to eliminate distinctions between protection of private communications based on arbitrary features of the technology used for transmission. Reflecting on technological developments of the 1980s with which the old Wiretap Act had failed to keep pace, the Senate Report on the ECPA lamented:
>
> > Today, we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing. A phone call may be carried by wire, by microwave or fiber optics. It can be transmitted in the form of digitized voice, data or video. Since the divestiture of AT & T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services. It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute.
>
> 1986 U.S.C.C.A.N. at 3556–57. It makes no more sense that a private message expressed in a digitized voice recording stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not.[342]

The court concluded by stating that Konop had raised material questions of fact concerning his claims of interception under the Federal Wiretap Act as well as his claims of unlawful access under the Stored Communications Act.[343] Very little of the court's opinion addressed the Stored Communications Act. But the court describes the Stored Communications Act as a lesser included offense of the Federal Wiretap Act.[344]

By affirming the reasoning of *Smith*, the court effectively held that someone who learns the contents of an electronic communication while it is in transmission or while it is held in electronic storage has intercepted that communication in violation of the Federal Wiretap Act. In

342. *Id.* at 1046.
343. *Id.* at 1048.
344. *Id.*

contrast, someone who unlawfully accesses a stored communications facility but does not proceed so far as to learn the contents of a stored electronic communication has merely violated the Stored Communications Act.

The court was absolutely correct in stating that an electronic communication in storage should be afforded the same level of privacy as an electronic communication in transmission. However, much of the statutory language is inconsistent with this assertion.

The Ninth Circuit's holding in *Konop I* reinforces *Smith's* implication that law enforcement officials would be bound exclusively by the more rigorous Federal Wiretap Act protections in seeking authorization to surreptitiously read a suspect's email. The Justice Department was aware that this result followed from *Smith* and *Konop I*. The Justice Department's Computer Crime Section stated that "[t]he decision in Konop is plainly incorrect: government access to electronic communications in 'electronic storage' is governed by 18 U.S.C. § 2703, not 18 U.S.C. § 2518."[345]

In *Konop II*, the Ninth Circuit reversed course, holding that violation of the Federal Wiretap Act occurs only where an electronic communication is intercepted while in transmission.[346] Thus, *Konop II* brings the Ninth Circuit in line with the Fifth Circuit's decision in *Steve Jackson Games*.

Konop II tried to distinguish the Ninth Circuit's earlier decision in *Smith,* explaining that *Smith* held that wire communications could be intercepted subsequent to transmission in violation of the Federal Wiretap Act, but did not go so far as to reach the same conclusion for electronic communication.[347] *Konop II* went on to correctly explain that *Smith* was effectively overridden by subsequent legislation. Section 209 of the USA PATRIOT Act of 2001 amended 18 U.S.C. § 2510(1) and 18 U.S.C. § 2703 to remove stored wire communication from the provisions of the Federal Wiretap Act and place it squarely within the Stored Communications Act.[348]

Moreover, *Konop II* recognized the Justice Department's criticism of *Konop I*. *Konop II* held that law enforcement efforts to view wire or electronic communications in storage at a provider of electronic communications service need only comply with 18 U.S.C. § 2703, explaining:

---

345. COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIM. DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, § IV. C. 2 (January 2001).

346. *Konop II*, 302 F.3d at 878.

347. *Id.* at 877–78.

348. 18 U.S.C.A. §§ 2150(1), 2703 (Supp. 2003). These statutory amendments will sunset and revert back to prior law on December 31, 2005.

> Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the [Stored Communications Act]. Congress could not have intended this result.[349]

Although *Konop II* reached the proper result according to the statutes, it unduly strained to avoid criticizing the rationale of *Smith*. *Konop II* asserted that *Smith*, like *Steve Jackson Games*, held that electronic communications in electronic storage could not be intercepted and so were governed exclusively by the provisions of the Stored Communications Act.[350] But despite some brief discussion to this effect,[351] crucial passages of *Smith* were devoted to explaining that violation of the Stored Communications Act is a lesser included offense of the Federal Wiretap Act.[352] *Smith* is reasonably interpreted as implying that it is a lesser included offense with regard to electronic communication as well as wire communication. If so, then stored electronic communications could be intercepted in violation of the Federal Wiretap Act. This was precisely the way that *Konop I* interpreted *Smith*.

The *Smith* and *Konop I* interpretation of the statutes as applied to stored electronic communication was not affected by the USA PATRIOT Act amendments,[353] which merely made clear that Federal Wiretap Act protections are not applicable to stored wire communications such as voicemail. To the extent that the Ninth Circuit approves the reasoning of *Smith*, *Konop I* follows more logically than *Konop II*. But even though the Ninth Circuit was unwilling to expressly disavow the rationale of *Smith*, *Konop II* has effectively done so.

In his partial dissent to *Konop II*, Judge Reinhardt contends that a stored electronic communication can be intercepted in violation of the Federal Wiretap Act.[354] He finds no justification for defining "intercept" so as to limit it to the contemporaneous acquisition of electronic communications.

By way of introduction, he raises an interesting question:

---

349. *Konop II*, 302 F. 3d at 879.
350. *Id.* at 878.
351. *United States v. Smith*, 155 F.3d 1051, 1057 (1998).
352. *Id.* at 1058–59.
353. *See* USA Patriot Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 (2001).
354. *Konop II*, 302 F.3d at 886–87 (Reinhardt, J., dissenting).

> Because I recognize that any reading of the relevant statutory provisions raises some difficulties and introduces some inconsistencies, the question becomes: which reading is more coherent and more consistent with Congressional intent?[355]

If the issue is presented as a question of statutory construction, then the majority opinion is more consistent with legislative intent because it avoids the scenario where law enforcement officials are required to comply with the Federal Wiretap Act to learn the contents of stored email, while the Stored Communications Act becomes irrelevant. But the courts have yet to answer the question of whether the constitutional protections of *Berger v. New York*[356] apply to stored email. If so, the Stored Communications Act limitations on covert police searches are insufficient to satisfy the constitutional safeguards that were expressed in *Berger*.

VI. INTERCEPTION OF EMAIL AND THE "CARNIVORE" CONTROVERSY

The July 11, 2000 issue of the *Wall Street Journal* revealed the existence of software developed at an FBI laboratory in Quantico, Virginia for the purpose of monitoring communications over the Internet.[357] Known as "Carnivore" for its ability to get to the meat of a vast quantity of information, the software was designed to run on hardware that is hooked directly into an Internet Service Provider's network.[358]

The Carnivore software is installed on a personal computer, which in many cases is kept in a locked cage on the premises of the Internet Service Provider. Theoretically, Carnivore gives the FBI the ability to monitor all of the ISP's customers' email and web surfing, although it is intended to focus on the activities of a specified individual from among all of the messages passing through the ISP's network.[359]

The *Wall Street Journal* article reported that Robert Corn-Revere, an attorney with Hogan and Hartson, represented an unidentified ISP in a challenge to the installation of Carnivore. The ISP objected to giving law enforcement agents access to all email traffic on its system, but a

355. *Id.* at 887.
356. Berger v. New York, 388 U.S. 41 (1967).
357. Neil King Jr. & Ted Bridis, *FBI's Wiretaps to Scan Email Spark Concern*, WALL ST. J., July 11, 2000, at A3.
358. *Id.*
359. *Id.*

magistrate ruled in favor of the government and ordered the installation of Carnivore.[360]

Mr. Corn-Revere submitted prepared testimony before a subcommittee of the House Judiciary Committee on April 6, 2000. Providing more information than appeared in the *Wall Street Journal*, he explained that he represented an Internet Service Provider in an attempt to quash an order authorizing U.S. Marshals to install the equivalent of a pen register and trap and trace device on its network.[361] The order called for the Marshals to obtain date, time, and addressing information regarding email sent to or from a particular email account.[362]

Initially, a U.S. Marshal told a representative of the ISP that the Marshals would install commercially available networking software known as "EtherPeek" on the ISP's network. The ISP was concerned about the capability of the software to actually view the contents of all email messages that were sent or received over its system.[363]

The ISP suggested a compromise whereby the ISP designed a software solution that would give the Marshals the necessary information without installing the EtherPeek software. The Marshal's Service initially agreed, but became dissatisfied with the compromise and insisted on installation of its own software. The ISP then filed a motion asking the Magistrate to quash or modify his order.[364]

In its opposition to the motion, the government explained that it no longer intended to install EtherPeek. Rather, it planned to install proprietary software called "Carnivore." The government acknowledged that Carnivore was capable of recording more information than was called for by the magistrate's order, but would be programmed not to do so. The government also conceded that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of its agents. The magistrate denied the ISP's motion, holding that the Marshal's actions amounted to the functional equivalent of a telephone pen register and trap and trace device.[365]

After the *Wall Street Journal* article was printed, Carnivore was the subject of enormous criticism in the press. Undoubtedly, the ominous

360. *Id.*

361. *Fourth Amendment and the Internet: Hearing Before the Subcommittee on the Constitution of the Committee on the Judiciary, House of Representatives*, 160th Cong. 73–75 (April 6, 2000), *available at* LEXIS, Federal News Service, LEGIS; FEDNEW (prepared Testimony of Robert Corn-Revere, Hogan & Hartson, L.L.P.) [herinafter Corn-Revere testimony].

362. *Id.*

363. *Id.*

364. *Id.*

365. *Id.*

sounding name contributed to the negative publicity and Carnivore was eventually renamed "DCS1000".[366]

In a July 11, 2000 letter to Hon. Charles Canady and Hon. Melvin Watt, members of the House Judiciary Committee's Subcommittee on the Constitution, the American Civil Liberties Union expressed concern about the means of operation of Carnivore. Citing to the article in the *Wall Street Journal,* the ACLU articulated its objections as follows:

> [U]nlike the operation of a traditional pen register, trap and trace device, or wiretap of a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP's network, not just the communications to or from a particular target. Carnivore, which is capable of analyzing millions of messages per second, purportedly retains only the messages of the specified target, although this process takes place without scrutiny of either the ISP or a court.
>
> Carnivore permits access to the email of every customer of an ISP and the email of every person who communicates with them. Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the "assurance" that the FBI will record only conversations of the specified target. This "trust us, we are the Government" approach is the antithesis of the procedures required under our the [sic] wiretapping laws. They authorize limited electronic surveillance of the communications of specified persons, usually conducted by means of specified communications devices. They place on the provider of the communications medium the responsibility to separate the communications of persons authorized to be intercepted from other communications.
>
> Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. Carnivore is not a minimizing tool. Instead, Carnivore maximizes law enforcement access to communications of non-targets.[367]

366. Erich Luening, *FBI takes the teeth out of Carnivore's name*, CNET NEWS.COM, February 9, 2001, *at* http://news.com.com/2100-1023-252368.html (last visited November 23, 2003).

367. Letter from Laura W. Murphy, Director ACLU Washington National Office, *et al.*, to Hon. Charles T. Canady and Hon. Melvin L. Watt, U.S. House of Representatives Committee on the Judiciary, Subcommittee on the Constitution (July 11, 2000), *available at* http://archive.aclu.org/congress/l071100a.html (last visited November 23, 2003).

The ACLU position is unpersuasive in arguing that wiretapping law requires the communications provider, rather than law enforcement officials, to separate the communications of the subject of the investigation from the communications of everyone else. To the contrary, the Federal Wiretap Act at 18 U.S.C. § 2516(3)[368] grants power to a judge to authorize "the interception of electronic communications by an investigative or law enforcement officer." 18 U.S.C. § 2518(4) adds that "an order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service . . . shall furnish the applicant forthwith all . . . technical assistance necessary to accomplish the interception unobtrusively."[369] Thus, the statute contemplates that interception will be accomplished by law enforcement officers, but gives them the option to demand assistance from the communication service provider.

As a practical matter, law enforcement officers may often rely on the communication service provider to execute the search, but they are not required to do so by statute. The safeguards of the Federal Wiretap Act do not charge the communication service provider with the primary responsibility to intercept email as a means to prevent abuses by law enforcement. And law enforcement officers who shift too much responsibility to the communication provider may run afoul of the Fourth Amendment, although case law to this effect has been overruled by statute.[370]

Moreover, the ACLU position fails to recognize the technological differences between conventional wire telephones and electronic communications over the Internet. Mr. Corn-Revere's statement to the Subcommittee on the Constitution correctly explained that a telephone call over a traditional circuit-switched telephone network creates a con-

368. 18 U.S.C. § 2516(3) (2000).

369. 18 U.S.C. § 2518(4) (2000). However, 18 U.S.C. § 2703(a) authorizes the government to require the provider of electronic communication service to disclose the contents of wire or electronic communication held in electronic storage. Apparently, the statute envisions the electronic communications service provider, rather than law enforcement officers, as having primary responsibility for executing a search for stored communications.

370. *See* United States v. Bach, No. CRIM.01-221 PAM/ESS, 2001 WL 1690055 (D.Minn. Dec. 14, 2001), *rev'd* 310 F.3d 1063 (8th Cir. 2002) (Minnesota police officers faxed a search warrant to Yahoo calling for certain email messages in a person's mailbox). The district court decision is troubling because it would require police officers to travel cross-country in order to execute a warrant even though they are not qualified to provide meaningful supervision to ISP employees. 18 U.S.C. § 2703(g) has been amended to expressly state that the presence of an officer is not necessary during service or execution of a search warrant seeking disclosure of the contents of communications by a provider of electronic communications service. Pub. L. No. 107-273, § 11010, 116 Stat. 1758 at 1822 (2002).

nection that is dedicated entirely to that conversation.[371] But the Internet is a packet-switched network that operates without a single, unbroken connection between the sender and the receiver. Information sent over the Internet is broken into many small packets that are reassembled in the proper order when they are received at the destination.[372]

The differences in communications technology dictate that the FBI use software known as a "packet sniffer" in order to establish a pen register, trap and trace device, or wiretap involving communications over the Internet.[373] The software searches for packets whose headers contain the email address of the sender or receiver under investigation and copies that information as called for in the pen register or trap and trace order. The software is also capable of copying the entire contents of the message as authorized in a wiretap order. Copied information is stored on an Iomega Jazz drive. Every day or two, an FBI agent removes the Jazz cartridge and inserts a new one.[374]

The ACLU's concern that the packet sniffer can read all of the email on an ISP's network is unfounded. Although Carnivore reads the headers of all messages passing through the ISP's network, the software only recognizes those messages where the sender or receiver is subject to investigation and copies the necessary information to disk. All other messages traveling across the network are ignored. It is difficult to find an invasion of privacy when the packet sniffer harmlessly reads the headers of email not subject to a surveillance order but retains no information from that message and makes no record of the fact that the message was ever sent.

While it is possible that FBI agents could program Carnivore to record all email on the ISP's network, it is unlikely that they could do so without being discovered. According to the man who designed the software, an attempt to record so much email would require the cooperation of too many people, including employees of the ISP, to maintain the secrecy of the effort.[375]

However, Mr. Corn-Revere's Congressional testimony pointed out two significant concerns about the implementation of Carnivore. First, a packet sniffer such as Carnivore has access to message routing information and actual content because both are contained in the packets. So it is possible that Carnivore could be configured to reveal content

371. Corn-Revere testimony, *supra* note 361, at 73.

372. *Id.*

373. Ted Bridis & Neil King, Jr., *Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000 at A28; Jeff Tyson, *How Carnivore Works*, ABOUT.COM, *at* http://computer.howstuffworks.com/carnivore.htm (last visited November 23, 2003).

374. Tyson, *supra* note 373.

375. Bridis & King, *supra* note 373.

when a court has only authorized the FBI to obtain routing information. Mr. Corn-Revere noted the potential for abuse when a pen register can easily be modified to obtain message content beyond the scope of judicial authorization.[376]

Second, at the time of Mr. Corn-Revere's testimony, the pen register and trap and trace statute used language envisioning a physical connection on a traditional telephone line rather than packet sniffing on a computer network.[377] Mr. Corn-Revere suggested that Congress should consider updating the statute in light of new technologies.[378]

While much concern has been expressed about the technical capabilities of Carnivore, less has been written about application of the statutory limitations imposed upon it. This article has pointed out in detail the restrictions imposed by the Federal Wiretap Act on law enforcement officers seeking to intercept email during the course of transmission. In contrast, the Stored Communications Act imposes substantially lesser restrictions on law enforcement officers seeking access to stored email that has already reached the recipient's mailbox.

Since Carnivore functions by intercepting email, law enforcement officers who employ Carnivore to learn the contents of email are bound by the rigorous safeguards of the Federal Wiretap Act. If law enforcement officers employed software that copied incoming email after it reached the recipient's mailbox and outgoing email while momentarily queued up before being released for transmission to the recipient, the lesser restrictions of the Stored Communications Act would govern. In this light, the FBI should be commended by privacy advocates for using technology that subjects its agents to the rigorous standards of the Federal Wiretap Act.

The obvious concern of privacy advocates is the potential for abuse of software like Carnivore whereby law enforcement agents view the contents of email beyond the scope of judicial authorization. Recognizing the extent of public concern about this issue, the Justice Department commissioned an independent study of the capabilities of

376. Corn-Revere testimony, *supra* note 361, at 73.

377. *Id.* The statute was subsequently revised by sec. 216 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 288–90 (2001).

378. Corn-Revere testimony, *supra* note 361, at 73.

Carnivore.[379] The Request for Proposals was released on August 24, 2000.[380]

The Request for Proposals quickly became controversial in its own right. Some researchers questioned whether an independent analysis could be conducted pursuant to the terms of the RFP. As a result, Massachusetts Institute of Technology, Purdue University, Dartmouth College, the University of Michigan, and the Supercomputing Center at the University of California at San Diego reportedly chose not to submit proposals.[381]

On September 6, 2000, the Department of Justice announced that it had selected the Illinois Institute of Technology Research Institute to perform the technical review of Carnivore.[382] IITRI issued a draft report dated November 17, 2000[383] and a final report dated December 8, 2000.[384]

The final report concluded that:

> Carnivore represents technology that protects privacy and enables lawful surveillance better than alternatives such as commercially available sniffer software. Carnivore restricts collected information in a precise manner that cannot be duplicated by other means. Although certain of Carnivore's functions could be duplicated by commercial products, there is no incentive to do so. The legitimate market for such a product is limited to law enforcement—a market already served by Carnivore. Moreover, publicly available products, such as EtherPeek, . . . are not capable of limiting collection as precisely as most court orders require, resulting in over-collection

379. *See* U.S. DEP'T JUSTICE, EXECUTIVE SUMMARY, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM, *at* http://www.epic.org/privacy/carnivore/RFP_exec_summ.pdf (last visited November 23, 2003); U.S. DEP'T JUSTICE, SOLICITATION, OFFER, AND AWARD, *at* http://www.epic.org/privacy/carnivore/RFP.pdf (last visited November 23, 2003).

380. Cecily Barnes, *DOJ Sets Rules for Carnivore Wiretap Investigation*, CNET NEWS.COM, August 24, 2000, *at* http://news.com.com/2100-1023-244937.html (last visited November 23, 2003).

381. Cecily Barnes, *DOJ Picks University to Study Carnivore*, CNET NEWS.COM, September 26, 2000, *at* http://news.com.com/2100-1023-246250.html (last visited November 23, 2003).

382. *Id.*

383. STEPHEN P. SMITH, ET AL., INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM, DRAFT REPORT, *at* www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (November 17, 2000) (last visited November 23, 2003) (some material was redacted from the publicly available version. *See* http://www.usdoj.gov/jmd/publications/carniv_entry.htm (last visited November 23, 2003)) [hereinafter DRAFT REPORT].

384. STEPHEN P. SMITH, ET AL., INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM, FINAL REPORT, *at* http://www.epic.org/privacy/carnivore/carniv_final.pdf (December 8, 2000) (last visited November 23, 2003) [hereinafter FINAL REPORT].

> and greater reliance on human intervention to minimize the information collected.[385]

The report recognized that Carnivore has the ability to over-collect data beyond the scope of judicial authorization. The agent who sets up Carnivore must select the proper filters to ensure that only the data called for in the court order is recorded. Procedural safeguards minimize the possibility of error because "multiple agents, FBI technical advisers, and often ISP personnel must agree on the settings before Carnivore is turned on."[386]

The report also noted that when used as a pen register/trap and trace device to record the sender and receiver of email, Carnivore arguably collects more information than is authorized.[387] Carnivore properly captures the contents of the "TO" and "FROM" fields of an email message. But it replaces characters in other fields with the letter "X". Thus, agents can determine the length of a message, but not the content.[388] In this regard, Carnivore may be out of compliance with 18 U.S.C. § 3121(c), which requires a government agency to use reasonably available technology so as to prevent a pen register/trap and trace device from recording anything other than dialing or addressing information.[389]

The report downplays the possibility that Carnivore can spy on all email users across the ISP's network because the volume of data would quickly fill up the storage media on the computer running the software.[390] More seriously, the report points out that the Carnivore software does not require each agent to log in with a unique ID in order

---

385. *Id.* ¶ 4.2.1, at 4-2.

386. *Id.* ¶ 4.2.3, at 4-3.

387. *Id.* ¶ 4.3.1, at 4-9.

388. *Id.* The ability to measure the length of a message goes beyond the scope of a traditional telephone pen register/trap and trace device. This feature constitutes a further invasion of privacy because it goes to the content of the message in question. For example, it has been pointed out that:

> This data may seem insignificant, but consider the following hypothetical: A judge authorizes FBI agents to use Carnivore to capture e-mail addresses sent to and from a person suspected of violating child pornography laws. While the agents are viewing this information, they notice most messages are small but some are extraordinarily large, perhaps indicating that illegal pictures are being transmitted. Therefore, in some cases the FBI has the ability to ascertain, or at least accurately guess, the nature of an e-mail without first obtaining Title III authorization.

Manton M. Grier, Jr., Comment, *The Software Formerly Known as "Carnivore": When does E-Mail Surveillance Encroach Upon a Reasonable Expectation of Privacy?*, 52 S.C. L. REV. 875, 886–87 (2001).

389. 18 U.S.C. §3121(c) (2000); *see* Rosow, *supra* note 102, at 1062.

390. FINAL REPORT, *supra* note 384, ¶ 4.2.3, at 4-4.

to change any of the filter settings. So it is not possible to ensure individual accountability for such changes.[391] The report is quite extensive and contains much more information than will be summarized here.

In actual use, it was widely reported that Carnivore overcollected information on at least one occasion involving a terrorism investigation conducted by the unit within the FBI that investigates activities of al Qaeda. The reports originated from the Electronic Privacy Information Center, which obtained an internal FBI memo[392] pursuant to a Freedom of Information Act request. According to an EPIC press release,[393] the memo reveals that Carnivore not only captured the email of the target of the investigation, but also included email of other people beyond the scope of judicial authorization. The memo also reveals that the agent conducting the surveillance was so upset that he destroyed all of the captured email, including the messages whose interception was judicially authorized.[394]

This episode serves as a reminder that technology will occasionally malfunction. Moreover, it is unlikely that technology can entirely prevent human error or intentional misconduct on the part of the police. In the final analysis, society must place a certain amount of trust in the competence and integrity of law enforcement officials. If that trust is violated, they must be held accountable. But outright rejection of Carnivore and the underlying packet sniffing technology for fear of potential abuse would unduly limit necessary law enforcement operations. However, as is true of all software, Carnivore is subject to modification and new versions may be created by the FBI. It would be prudent to provide for a periodic independent review of the software to ensure that appropriate operational safeguards are not lost in the upgrade process.[395]

391. *Id.* ¶ 4.2.4, at 4–5.

392. Memorandum from unknown person, to Spike Bowman at the FBI (April 5, 2000), *available at* http://www.epic.org/privacy/carnivore/fisa.html (last visited November 23, 2003).

393. Press Release, Electronic Privacy Information Center, FBI's Carnivore System Disrupted Anti-Terror Investigation (May 28, 2002), *available at* http://www.epic.org/privacy/carnivore/5_02_release.html (last visited November 23, 2003).

394. An FBI spokesman said that the memo is incorrect. The emails were retained and remain under seal. Dan Eggen, *"Carnivore" Glitches Blamed for FBI Woes; Problems with e-Mail Surveillance Program Led to Mishandling of al Qaeda Probe in 2000 Memo Says*, WASH. POST, May 29, 2002, at A7.

395. FINAL REPORT, *supra* note 384, ¶ 5.9, at 5-4.

VII. ENCRYPTED EMAIL AND KEYSTROKE LOGGERS

Carnivore enables law enforcement officers to intercept email and read its contents. However, email that has been encrypted poses additional difficulties. Although Carnivore can intercept encrypted email, the contents cannot be read without the proper "key." In order to read encrypted email, law enforcement officers must employ additional technologies to surreptitiously obtain the key.

Cryptography software garbles a message through a mathematical formula known as an encryption algorithm so that only the sender and the receiver, who are in possession of the key, can read it. The key can be a number, a word, or a phrase. The key operates as a password. When the receiver enters the proper key, the encryption algorithm decrypts the message.[396]

Pretty Good Privacy (PGP) is a popular and effective encryption program based on a type of encryption known as public key cryptography. The software generates a public key and a private key for an individual. This person would make his public key generally available to the world, but would maintain the secrecy of his private key.

By way of example, suppose Sender wants to send a secure email message to Receiver. Sender uses the software and Receiver's public key to encrypt the message before emailing it to Receiver. When the message arrives, Receiver then uses the software and his private key to decrypt the message.[397]

The first known judicial decision addressing FBI efforts to covertly obtain and decrypt encrypted files is *United States v. Scarfo*.[398] Scarfo was suspected of following in his father's footsteps as an organized crime figure.[399] As part of an investigation into illegal gambling and loan-sharking, the FBI obtained a warrant to surreptitiously search Scarfo's office for evidence. During the search, FBI agents copied files

396. *See* SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY 34–39 (1995). It is possible, but very difficult, to decrypt an encrypted message without the key. To prove a point, the Electronic Frontier Foundation conducted an experiment involving a well-known encryption algorithm called "DES." As of 1995, it was believed that a computer capable of decrypting a DES-encrypted message within a few hours could be built for approximately $1 million. But no government or corporation would admit to owning such a computer. In 1998, the Electronic Frontier Foundation built a computer that could decrypt a DES-encrypted message in 3 days at a cost of $220,000. Having completed the basic research, the Electronic Frontier Foundation could build another computer for $50,000. *Id.* at 43; *See* Randy Weston, *Group Cracks Crypto Standard*, CNET NEWS.COM, July 17, 1998 *at* http://news.com.com/2100-1023-213461.html?legacy=cnet&tag=st.cn.1fd2 (last visited November 23, 2002).

397. GARFINKEL, *supra* note 396, at 47–50.

398. 180 F. Supp. 2d. 572 (D.N.J. 2001).

399. Jonathan Krim, *High-Tech FBI Tactics Raise Privacy Questions*, WASH. POST, August 14, 2001, at A1.

found on Scarfo's computer, but discovered that a file named "Factors" was encrypted through Pretty Good Privacy software and could not be read.[400]

The agents subsequently returned to the office pursuant to another warrant authorizing them to place a keystroke logger on Scarfo's computer. The keystroke logger records the keystrokes entered on the computer's keyboard. The FBI eventually obtained the password and retrieved incriminating evidence from the file.[401]

The Government has revealed few details about the manner in which the keystroke logger operates. It is not even known whether the logger is a software program or a hardware device. At trial, Scarfo sought discovery and moved to suppress the evidence obtained from his computer. The court was particularly troubled by the possibility that use of the keystroke logger by the FBI violated the Federal Wiretap Act. The court explained:

> In an August 7, 2001, Letter Opinion and Order, this court expressed serious concerns over whether the government violated the wiretap statute in utilizing the [keystroke logger] on Scarfo's computer. Specifically, the Court expressed concern over whether the [keystroke logger] may have operated during periods when Scarfo (or any other user of his personal computer) was communicating via modem over telephone lines, thereby unlawfully intercepting wire communications without having applied for a wiretap pursuant to Title III, 18 U.S.C. § 2510.[402]

The court ordered the government to file a report explaining the technology behind the keystroke logger and addressing its ability to operate while the modem was in use. But the government argued that disclosure of the information would jeopardize national security interests and requested an *in camera*, *ex parte* hearing pursuant to the Classified Information Procedures Act of 1980.[403] After conducting the hearing, the court permitted the government to merely provide Scarfo with an unclassified summary of the information related to the keystroke logger. The court believed that the summary was sufficient to

400. *Scarfo*, 180 F. Supp. 2d at 574.

401. *Id.* The password turned out to be the prison identification number of Scarfo's father. Krim, *supra* note 399.

402. *Scarfo*, 180 F. Supp. 2d at 575.

403. 18 U.S.C. Appendix III, §§ 1–16 (2000). However, keystroke loggers are available commercially. Karen J. Bannan, *Watching You, Watching Me*, PC MAGAZINE, July 2002, at 99.

allow Scarfo to challenge the admissibility of the evidence taken from his computer.[404]

The court ultimately held that the FBI did not intercept a communication in the course of transmission over the telephone lines.[405] Therefore, the warrant obtained by the FBI was sufficient to authorize use of the keystroke logger. The FBI was not required to obtain authorization under the Federal Wiretap Act.[406]

The court reached this conclusion based on the affidavit of an FBI official, who explained that the FBI "did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer."[407] In other words, the FBI configured the keystroke logger "to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communications ports."[408]

However, it has been pointed out that "even if the key logger didn't intercept communication after it was sent by the computer's modem, it effectively does the same thing by capturing what is typed on an e-mail or instant message form just before the user hits the send button."[409] This issue highlights a fundamental flaw underlying the rationale of the wiretapping statutes. If the FBI agents had intercepted Scarfo's communications during transmission, they would have been bound by the detailed safeguards of the Federal Wiretap Act. But where the FBI surreptitiously obtained the same material directly from Scarfo's computer, they were merely bound by the less rigorous safeguards against surreptitious searches generally as per Federal Rule of Criminal Procedure 41, which did not expressly address sneak and peak searches at that time.[410]

Yet it can be persuasively argued that a person's privacy interest in a file on his computer (or a paper document in his desk) behind locked office doors is equivalent to the privacy interest in a telephone call or an email message. If so, that electronic file or paper document locked up in a closed office should be afforded the same protection from surreptitious searches by law enforcement officers.

---

404. *Scarfo*, 180 F. Supp. 2d at 575–76.
405. *Id.* at 581.
406. *Id.* at 581–82.
407. *Id.* at 581.
408. *Id.* at 581–82.
409. Krim, *supra* note 399.
410. Subsequently, the USA PATRIOT Act amended 18 U.S.C. § 3103a to provide some additional guidance as to the procedures regulating sneak and peak searches. *See supra* note 60 and Part V.C.

Moreover, the "Factors" file on Scarfo's computer that was obtained covertly by law enforcement officers was not said to have ever been communicated to anyone by Scarfo. The privacy interest in material locked in a person's home or office where the owner sought to maintain total secrecy is arguably greater than the privacy interest in a phone call, where a party to a telephone conversation is revealing information to at least one other person.

But the similarity between privacy interests is often neglected because telephone wiretaps must always be conducted covertly, while searches of files in a desk or on a computer are most often conducted with contemporaneous notice to the owner. It is reasonable to set lower safeguards governing search and seizure with contemporaneous notice because a lesser invasion of privacy arguably occurs when the execution of the search is not hidden from the property owner. But this article asserts that the invasion of privacy taking place when the police covertly break into a home or office to conduct a search is equivalent to the invasion of privacy taking place when the police covertly conduct a wiretap so the procedural safeguards should be the same.

Nevertheless, the statutes provide the greatest level of protection to a telephone call. This discrepancy in the level of protection from surreptitious searches illustrates the shortcoming of a technology-based analysis. Rather than looking to the technology to determine the level of protection from covert searches by law enforcement officers, Congress should focus on the underlying privacy interest that exists regardless of technology and medium of communication. The underlying privacy interest at issue when the police employ a low-technology covert entry into a house to search for paper documents is the same as the privacy interest at issue when the police conduct a high-technology wiretap of a person's telephone.

Once again, it is interesting to look back at how this area of law has evolved since *Olmstead*[411] was decided in 1928. Back then, the Supreme Court was willing to provide safeguards against an intrusion into a person's home or office, but was not willing to recognize a privacy interest in a telephone call traveling over the telephone lines. Today, the statutes create stringent safeguards to protect telephone calls and email messages traveling over the telephone lines or the Internet, but afford significantly lesser protections against the FBI secretly entering a locked home or office to search for communications and other documents stored on a computer.

411. 277 U.S. 465 (1928).

VIII. TOWARD A UNIFORM PROCEDURE GOVERNING SURREPTITIOUS SEARCH AND SEIZURE

This article has discussed the stringent procedural requirements that must be satisfied before law enforcement officials can lawfully conduct a telephone wiretap. These requirements originated in *Berger v. New York*[412] and were codified along with additional safeguards in the Federal Wiretap Act.[413] But the courts have never adequately explained why such rigorous standards apply uniquely to telephone wiretaps.[414]

In 1928, Justice Brandeis asserted that a telephone wiretap constitutes a greater invasion of privacy than interception of a letter in the mail because a wiretap invades the privacy of both parties to the conversation, and potentially intrudes upon discussion that is unrelated to criminal activity.[415] Wiretapping of a person's telephone also eavesdrops on conversations with everyone he calls and everyone who calls him.[416]

But the same is true for the covert search of an ongoing exchange of postal mail or email between the person under surveillance and the people he communicates with. So Justice Brandeis' observation does not account for the distinctions that developed in the law governing covert searches of postal mail or email.

The unstated assumption of *Berger* seems to be that the real-time, covert interception of a telephone conversation by law enforcement officials somehow constitutes a greater invasion of privacy than a covert search of other media of private communications and so should be subject to greater safeguards. Such an assumption is consistent with enactment of the Federal Wiretap Act in 1968, where Congress did not broadly draft the statute to provide the same protection against covert interception of letters in the mail. And the assumption was implicit in the 1986 Federal Wiretap Act amendments applicable to the interception of electronic communication (which afforded less protection than was afforded to wire communication) as well as the Stored Communications Act governing stored wire and electronic communications (which were afforded even less protection).

This article questions that assumption. This article argues that precisely the same privacy interest is implicated regardless of whether the surreptitious search of a communication takes place in real-time and regardless of the medium of communication so long as the communica-

412. 388 U.S. 41 (1967).
413. *See* 18 U.S.C. §§ 2510–2522 (2000).
414. *See supra* Part V.A.
415. Olmstead v. United States, 277 U.S. 438, 475–76 (1928).
416. *Id.*

tions technology is reasonably designed to avoid unintentional interception by third parties.

In other words, the Fourth Amendment and the applicable statutes should provide the same level of protection from covert searches to any medium of communication that is deemed worthy of protection at all and the same procedural safeguards should govern. Thus, *Berger* would be better interpreted as focusing on the surreptitious nature of the invasion of privacy rather than on the real-time nature of the medium of communication. But *Berger* has not been so construed, and the statutory codification of *Berger* has not been so far-reaching.

By way of comparison, the courts have long held that search and seizure of a letter in the mail must be based on a judicially issued search warrant supported by probable cause. As early as 1877, the Supreme Court recognized that Fourth Amendment protections apply to letters in the mail just as they apply to papers retained in the sender's home.[417]

However, the situation becomes more complicated where law enforcement officials secretly intercept an ongoing stream of mail without contemporaneous notice to the subject of the investigation. The stringent *Berger* standards have never been applied where the medium of communication is conventional postal mail. Rather, the lesser protections of Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 3103a govern. This article asserts that the privacy interest in postal mail is equivalent to the privacy interest in telephone conversations and both are deserving of the same protection against covert searches despite the real-time nature of the telephone.

It would not be unreasonable to expand the *Berger* standards and the statutory protections for wire communications to govern all covert searches for private communications or personal documents. The Ninth Circuit's decision in *Freitas I* analogized the sneak and peak search to a telephone wiretap.[418] The court asserted that a showing of necessity in the application for a sneak and peak warrant would strengthen the government's argument that the covert search was conducted in compliance with the Fourth Amendment.[419] Even though the Ninth Circuit was willing to draw the analogy, the court was unwilling to go so far as to require a showing of necessity in order to obtain a sneak and peak warrant. In contrast, the Second Circuit's decision in *United States v. Villegas* imposed a standard of reasonable necessity to justify

417. Ex parte Jackson, 96 U.S. 727 (1877).

418. 800 F.2d 1451, 1456 (9th Cir. 1986) ("The surreptitious character of the search and seizure in this case calls to mind wiretapping. . . .").

419. *Id.*

a covert entry search.[420] A similar, but apparently less rigorous standard was recently codified by the USA PATRIOT Act.[421]

As new types of communications devices proliferate and gain in popularity, Congress continues to afford the greatest safeguards against covert surveillance to telephone conversations. Nevertheless, the history of the Federal Wiretap Act shows a continual struggle to apply the statute to emerging telephone technologies, often with unsound results.

For example, the Ninth Circuit concluded that a conversation taking place over two mobile phones was not necessarily protected by the Federal Wiretap Act as it existed at the time, while a conversation taking place between a conventional, wire telephone and a mobile phone would be protected. Other courts held that the wire portion of a portable telephone conversation was protected by the early language of the statute, but the broadcast portion of the conversation was not protected.[422]

In 1986, the Federal Wiretap Act was amended to protect cellular telephone conversations, but the statute expressly excluded the broadcast portion of portable telephone conversations.[423] It was not until 1994 that the exclusion of the broadcast portion of portable telephone conversations was deleted from the statute.[424]

Similarly, the Federal Wiretap Act amendments (and the Stored Communications Act as well) pertaining to electronic communications continue to unduly focus on technology rather than the underlying privacy interest. This undue emphasis on the medium of communication likewise leads to unsound results when applying the statute to emerging Internet technologies. The problem derives in part from the underlying difficulty of classifying Internet technologies as real-time communications (which are arbitrarily afforded greater protections under the Federal Wiretap Act) or stored communications (which are arbitrarily afforded lesser protections under the Stored Communications Act). The issue is illustrated by the manner in which the two statutes treat email. It follows from *Steve Jackson Games*[425] that law enforcement officers who want to intercept email in real time during transmission must comply with the rigorous safeguards of the Federal Wiretap Act. Yet if they access that same message in electronic storage

420. 899 F.2d 1324, 1337 (2d Cir. 1990). In establishing a standard of reasonable necessity, *Villegas* expressly stated that the standard is not as rigorous as the requirement of the Federal Wiretap Act. *See supra* Part II.B.

421. 18 U.S.C.A. § 3103a (2003). *See supra* Part II.B.

422. United States v. Hall, 488 F.2d 193, 198 (9th Cir. 1973); *see supra* Part V.B.2.

423. 18 U.S.C. §§ 2510–2520 (Supp. IV 1986); *see supra* Part V.B.3.a.

424. *See supra* Part V.B.4.

425. 36 F.3d 457 (5th Cir. 1994).

after it reaches the recipient's mailbox, they need only comply with the lesser protections of the Stored Communications Act.[426]

It would be hard to characterize the underlying privacy interest in an email message as greater during the course of transmission than after it reaches the recipient's mailbox. Yet the statutes afford rigorous safeguards against the interception of email during transmission by law enforcement officers, while affording lesser protections against law enforcement access to email held in electronic storage in the recipient's mailbox at his Internet Service Provider.

In this regard, the drafters of the statutes did not anticipate a fundamental distinction between a telephone conversation and an email message. A telephone conversation can only be monitored while it is taking place, thereby giving rise to the real-time aspect of the wiretap. But email is not quite as ephemeral as a telephone conversation. Email can be intercepted while in transmission or accessed after it has actually reached the recipient's mailbox. Of course, the recipient can only read it after it has been stored in his mailbox, so in that sense it is misleading to talk about a real-time transmission of email because there is inevitably some delay before even the intended recipient can read it. This is the reason why the influential decision in *Steve Jackson Games* struggled with the question of whether email could be intercepted while in electronic storage. Actually, this question becomes moot if one accepts the argument that the privacy interest remains the same regardless of whether the email is intercepted during transmission or accessed from storage in the recipient's mailbox.

Poor statutory drafting has led to even greater difficulty in determining whether voicemail is capable of real-time interception. Until amended by the USA PATRIOT Act in 2001, the Federal Wiretap Act implied that voicemail can be intercepted for purposes of the statute. However, the Stored Communications Act implied that voicemail is merely accessed from storage, thereby losing the real-time immediacy of a telephone call and the rigorous statutory protections that are afforded to it. The Ninth Circuit was directly confronted with this discrepancy in *United States v. Smith*.[427] The court resolved the issue through a convoluted analysis leading to the conclusion that the Federal Wiretap Act governs the interception of voicemail.[428]

Although the Ninth Circuit reached a desirable result in affording the Federal Wiretap Act's greater protection to voicemail, it strained too far in trying to reconcile the clearly inconsistent language between

426. *See supra* Part V.C.1.
427. 155 F.3d 1051 (9th Cir. 1998).
428. *Id.* at 1058; *see supra* Part V.C.2.

the two statutes. Alternatively, the court should have simply acknowledged that the conflicting statutory provisions could not be reconciled and so the court applied the greater protection of the Federal Wiretap Act to voicemail.[429]

The reasoning of *Smith* was carried over into *Konop v. Hawaiian Airlines*,[430] which addressed the issue of whether a web page stored on a web server could be intercepted for purposes of the Federal Wiretap Act. If so, then the greater protections of the Federal Wiretap Act would come into play.

In the context of a civil lawsuit, *Konop I* held that an electronic communication could be intercepted even though it was already held in electronic storage. *Konop I* had serious implications for law enforcement because it leads to the conclusion that law enforcement officers must always comply with the strict procedural requirements of the Federal Wiretap Act in order to conduct a search for stored electronic communications. Accordingly, the more relaxed warrant provisions of the Stored Communications Act would be rendered irrelevant.[431]

Konop I was a logical extension of *Smith,* but the Ninth Circuit recognized its far reaching implications. *Konop I* was withdrawn. *Konop II* held that access to a stored electronic communication such as a web page is governed exclusively by the Stored Communications Act. *Konop II* brought the Ninth Circuit in line with the Fifth Circuit, which expressed the same view in *Steve Jackson Games.*

Konop I correctly stated that "an electronic communication in storage is no more or less private than an electronic communication in transmission."[432] It was also correct in asserting that "distinguishing between the two for purposes of protection from interception is 'irrational'."[433] Nevertheless, the statutes call for significant distinctions between them.

The arbitrary nature of the statutory distinctions will be magnified when applying the statutes to Internet telephony, where a personal computer can be used to talk to someone using another personal computer or a conventional telephone. Likewise, they will be exacerbated where the statutes determine the protections afforded to

429. USA PATRIOT Act amendments to the statutes provide that voicemail receives the lesser protections of the Stored Communications Act, but the statutory amendments are scheduled to sunset on December 31, 2005. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 (2001).

430. 236 F.3d 1035 (9th Cir. 2001) [*Konop I*], *opinion withdrawn by* 262 F.3d 972 (2001), *superseded* by 302 F.3d 868 (9th Cir. 2002) [*Konop II*], *cert. denied* 537 U.S. 1193 (2003).

431. *See supra* Part V.C.3.

432. *Konop I*, 236 F.3d at 1044–46.

433. *Id.*

communications via Personal Digital Assistants incorporating cell phone technology, and to cell phones featuring Internet access.[434] As society grows to view telephone and Internet technologies as essentially one and the same, any distinctions will become increasingly out of touch with the privacy expectations of the American public.

Further statutory deficiencies will come to light as law enforcement officials employ new surveillance technologies. *Scarfo*[435] provides yet another example of arbitrary results that follow from the current statutory scheme. There, the FBI did not intercept Scarfo's email. Rather, FBI agents covertly entered Scarfo's office and copied files directly from Scarfo's computer. When they saw that a file was encrypted, they surreptitiously returned and secretly installed a keystroke logger while no one was in the office. Subsequently, they returned again and, using data collected by the keystroke logger, discovered the encryption password needed to decrypt the file. These activities were all judicially approved by search warrants authorizing sneak and peak searches, but the FBI agents were not required to comply with the detailed safeguards of the Federal Wiretap Act.[436]

Once again, the statutory scheme yields a poor result by wrongly focusing on the issue of whether the FBI conducted a real-time interception of communications during transmission. The investigators were careful to avoid any such interception by configuring the keystroke logger to not record keystrokes while the modem was transmitting. Instead, the keystroke logger could record keystrokes moments before transmission and effectively make available the same information.[437] Since the keystroke logger did not provide the FBI with real-time information intercepted during transmission, the Federal Wiretap Act did not govern the search. And since the FBI accessed a document stored on a personal computer in a person's office rather than a document stored at an electronic communication service, the Stored Communications Act was likewise inapplicable. Rather, the only safeguards were the standards governing sneak and peak searches in general.

However, this article asserts that the privacy interest in an electronic document stored on a personal computer or a paper document

434. Under the current statutory scheme, the courts will need to determine whether those conversations amount to wire communications or electronic communications. In either case, the Federal Wiretap Act governs interception by law enforcement officers during transmission. Of course, this article has repeatedly asserted that the statute provides greater protections while communications are in transmission than when they are in storage, but the inquiry does not end there. The Federal Wiretap Act also provides greater protection for wire communication during transmission than for electronic communication during transmission.

435. 180 F. Supp. 2d. 572 (D.N.J. 2001).

436. *Id.* at 574, 581.

437. *Id.* at 581–82.

stored in a file cabinet locked in a person's office is deserving of at least as much protection from covert searches by law enforcement officials as is afforded to a telephone call. The privacy interest that is compromised when the police conduct a covert search remains the same regardless of whether the material seized exists in wire, electronic or paper format and regardless of whether the material is intercepted during transmission or accessed from storage. Therefore, the *Berger* standards should govern the decision whether to grant judicial authorization for the covert search. To the extent that the statutes expand upon the *Berger* safeguards to determine whether the courts will permit the police to implement a telephone wiretap, the statutes should likewise expand the safeguards in these other contexts as well.

Scarfo demonstrates the appropriateness of the *Freitas I* analogy between sneak and peak searches and telephone wiretaps. Scarfo clearly had a significant privacy interest in an encrypted document stored on a computer locked in his office and not knowingly revealed to anyone. Scarfo's expectation that the police will not covertly enter his office to learn the contents of the document is at least as great as his expectation that the same document, when attached to an email message, will not be covertly intercepted by the police during transmission to another person. Yet under the current statutory scheme, greater protection against a covert police search is afforded to a communication during transmission than is afforded to a document that remains locked in an office and is never communicated to anyone at all.

A better statutory scheme would provide uniform regulation of all covert police searches of documents and communications regardless of whether they exist on paper, in wire format, or in electronic format. Such regulation should be codified in a single chapter of the U.S. Code. There is no justification for giving a telephone call more protection than an email message. Likewise, there is no justification for giving an email message in the course of transmission more protection than a message stored in a mailbox at an Internet Service Provider or in a personal computer locked in a person's home.

This proposed statutory revision would focus on the invasion of privacy that takes place during the execution of a covert search, which is more significant than the current focus on the real-time nature of the search. Of course, it is not possible to objectively quantify a person's privacy interest in his personal computer or file cabinet as compared to his privacy interest in the telephone lines or his electronic mailbox. Nevertheless, the same privacy interest is compromised regardless of whether the communication is covertly intercepted in real time (as in the case of a telephone call) or whether covert access to the communi-

cation is delayed (as in the case of a letter in the postal mail or an email in electronic storage).[438]

The arbitrary distinctions that began with *Berger* and were subsequently expanded by statute are overdue for revision. A new scheme focusing on the underlying privacy interest should be implemented. The current scheme, with its focus on the medium of communication, will not yield good results because the legislative process cannot keep up with the pace of innovation in communications technology.

Justice Brandeis was correct in 1928 when he anticipated that technological advancement will enable the Government to employ tools of surveillance extending beyond wiretapping. He asserted that Fourth Amendment protections must be interpreted broadly so as to safeguard against new abuses that were not previously envisioned. Thus, Brandeis sought to protect the individual's "right to be let alone" without regard to the different technologies that might be employed by the Government to compromise that right.[439] His focus on the underlying privacy interest would be more workable than the statutes currently in force.

438. The proposed statutory revisions could be drafted to apply exclusively to covert searches for documents and communications, or could apply more broadly to all covert searches because the intrusion into privacy interests is so similar.

439. Olmstead v. United States, 277 U.S. 438, 472–74, 478 (1928); *see supra* Part IV.A.